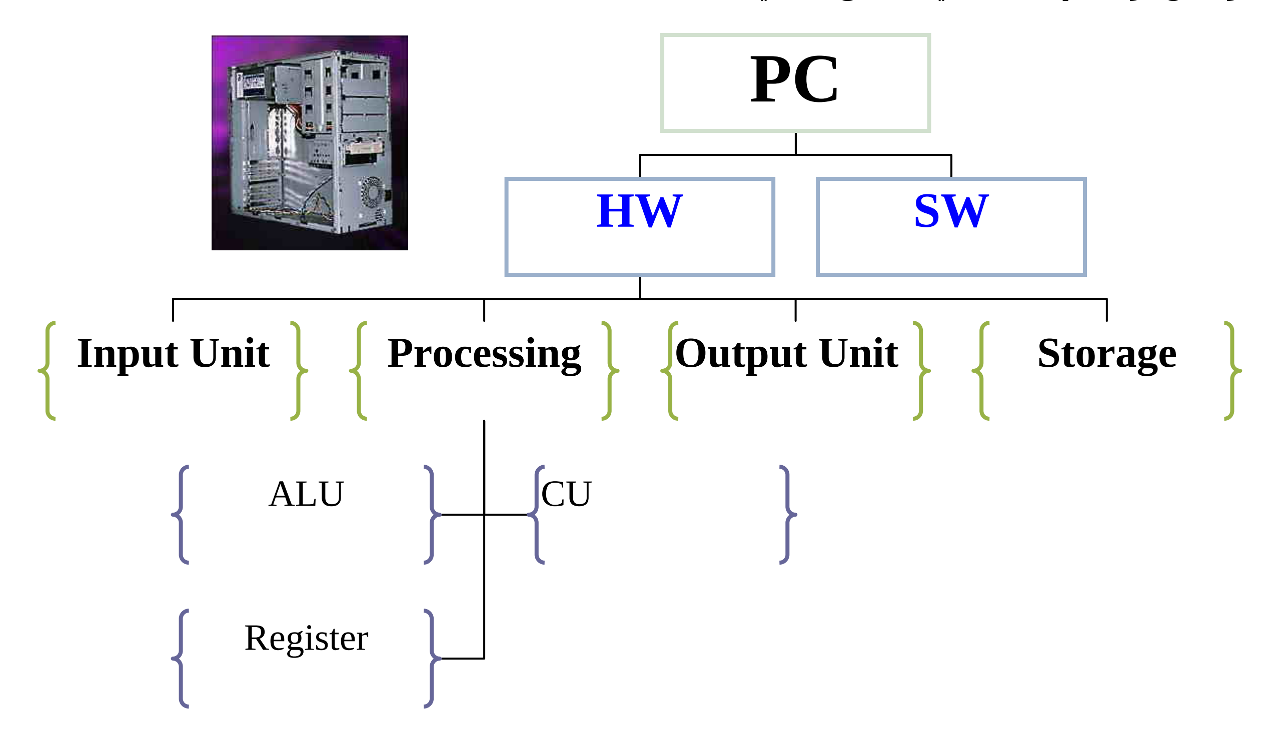
بسم الله الرحمن الرحيم

المحاضرة الأولى:
السبت 11-6-2005
مقدمة سريعة عن مفهوم الحاسوب :

جهاز الحاسوب PC يتكون من جزئين أساسيين وهما : السوفت وير Software والهارد وير Hardware ويمكن توضيحهما كما في الشكل التالي :



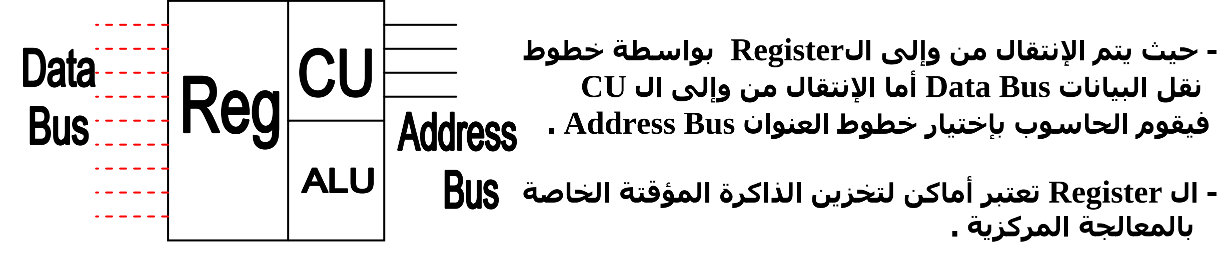
SW : هي البرمجيات التي تستخدم في جهاز الحاسوب وهي مجال ال Logical في الحاسوب حيث من خلال البرمجيات يتم بشكل أو بآخر التحكم بال HW .

HW : ينقسم إلى أربعة أقسام رئيسية كالتالي :

1 – وحدة الإدخال Input Unit :
وتتكون من أجهزة الإدخال إلى ال PC ، ومن الأمثلة عليها الماوس والكيبورد والسكانر ... إلخ .

2 – وحدة الإخراج Output Unit :
وتتكون من أجهزة الإخراج من ال PC ومن الأمثلة عليها الشاشة والطابعة ... إلخ .

3 – وحدة المعالجة المركزية Central Processing Unit المعروفة بال CPU :
- وحدة المعالجة المركزية مسؤولة عن تنفيذ تعاليم البرامج المختلفة .
- العمليات التي تقوم بها هذه الوحدة هي نقل البيانات و العمليات الحسابية والمنطقية والعلائقية وعمليات التحويل .
- كل معلومة يتم نقلها من وإلى ال CPU تنتقل على شكل نبضة إلكترونية إما صفر أو واحد .
- يوجد نوعين لروابك النقل وهما : Data Bus و Address Buss ويمكن تمثيلهم حسب إرتباطهم مع الـ CPU كما في الشكل التالي :



- حيث يتم الإنتقال من وإلى الRegister بواسطة خطوط نقل البيانات Data Bus أما الإنتقال من وإلى ال CU فيقوم الحاسوب بإختيار خطوط العنوان Address Bus .
- ال Register تعتبر أماكن لتخزين الذاكرة المؤقتة الخاصة بالمعالجة المركزية .

4 – وحدات التخزين Storage Unit :

وتنقسم إلى قسمين أساسيين وهما :

1 - الذواكر الرئيسية Main Memory .

2 - الذواكر الثانوية Secondary Memory .

- الذواكر الثانوية Secondary Memory : لأن الذاكرة الرئيسية ذات مصادر محدودة البرامج والبيانات تخزن في هذه الذواكر وخصوصاً إن كانت تستعمل لفترات طويلة ويتم تخزين المعلومات على شكل ملفات Files وميزتها أنها بطيئة لأنها بعيدة عن ال CPU وهي خاصة بال User أي أن عمليات الحفظ والطلب والإستدعاء تكون من إختصاصها ومن الأمثلة عليها : القرص المرن FDD و القرص الصلب HDD والقرص المضغوط CDD ... إلخ .

- الذواكر الرئيسية يراها المبرمجين أنها مجموعة من الخلايا تسمى Memory Cell وكل خانة منها يتم تخزين معلومات معينة . والخلية تختلف بإختلاف حجم الداتا التي تحملها ، فالتعاليم البرمجية يتم تخزينها في الذاكرة لتتفاعل مع وحدة المعالجة المركزية CPU .

- الذواكر الرئيسية Main Memory مهمة جداً لأن كل عمليات ال PC تتم فيها و يمكن تقسيمها إلى ثلاث أقسام جوهرية كالتالي :

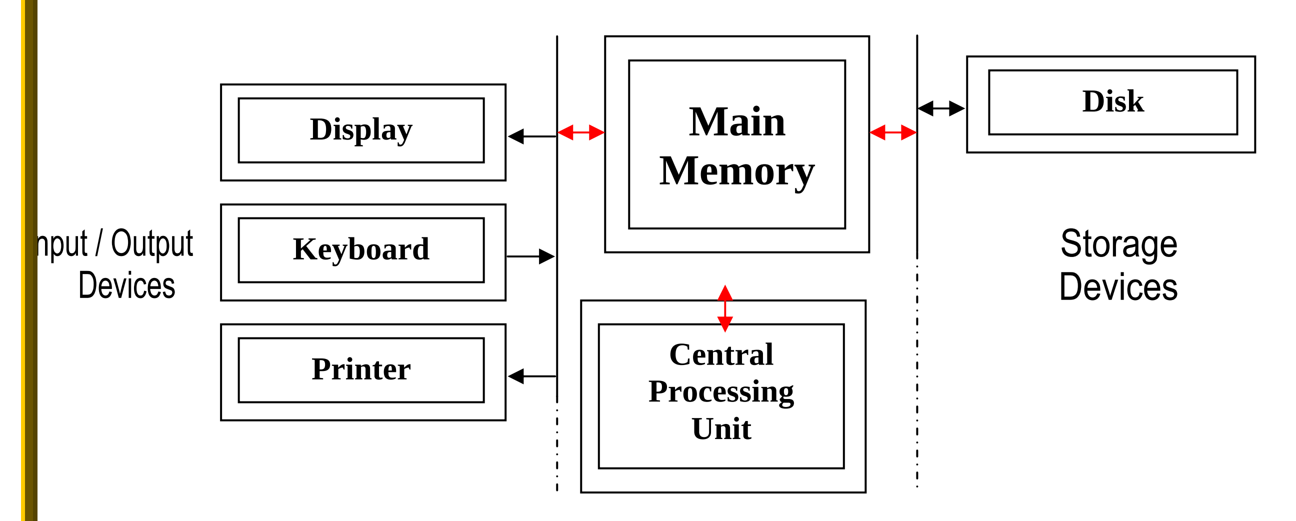
RAM – 1 ROM – 2 Cache – 3

- سنتعمق الآن في الذواكر الرئيسية كالتالي :

- ذاكرة الرام RAM :

- إختصار لجملة Random Access Memory أي الذاكرة العشوائية وسميت كذلك لأننا لو قمنا بإطفاء الجهاز تتلاشى كل الداتا التي بداخلها فهي ذاكرة تخزين لحظية .

- الرام يعتبر مرآة أو نظارة ال CPU أي أن ال CPU لا يتعامل ولا يأخذ إلا من الرام والعلاقة بينهما علاقة وطيدة إذا تعطلت الرام فال CPU لا يمكنه أداء وظيفته وسبب ذلك لأن ال CPU لا يأخذ المعلومات ولا يعطيها إلا للرام ويمككن توضيح ذلك كما في الشكل التالي :



- يقوم الرام بوضع خانات للبيانات وذلك بتخصيص الجزء الأول للعناوين بالترتيب ومن ثم تقوم بأخذ البيانات بشكل متسلسل حسب الترتيب الأولي .

- لماذا الرام ؟؟؟ في نقل البيانات لل CPU ؟

لأنها الأقرب لل CPU تعتبر الأسرع في نقل البيانات وهذه الميزة مهمة للعمليات وبذلك تتميز الرام عن وحدات التخزين المساندة مثل القرص الصلب أو المرن أو غيره .

وتنقسم الرام إلى نوعين من حيث مكوناتها :
1 - DRAM : وهي الرامات التي تصنع من المكثفات Capacitor وتقوم بتخزين الداتا إلكترونياً وهي تعتبر نوع مرن Dynamic ، وهو يقوم بإستهلاك طاقة أعلى .

2 - SRAM : وهي الرامات التي تصنع من الترانزيزتور TRANSISTOR وتستخدم البوابات المنطقية Logic Gates عن طريق الفليب فلوب Flip Flop لتخزين الداتا وهي تعتبر نوع ثابت Static، مقتصدة للطاقة الكهربائية .

3 - SDRAM : دمج بين النوعين DRAM والنوع SRAM وذلك لجعلها مرنة ومقتصدة للطاقة .

- أما بالنسبة لتكنولوجيا الرام فتنقسم إلى ثلاثة أقسام :
1 – SIMM : وهي إختصار لجملة Single Inline Memory Module ، ويقوم هذا النوع بنقل الداتا بت بت Bit By Bit وتتكون من 30 إلى 77 Pin (دبوس) وسرعتها 66 MHz ، وإنقرضت مع إنقراض البينتيوم 1 .

ويمكن تمثيل شكلها بالرسم التالي :
أي أنها تتميز بزاوية غير معكوفة .



2 – DIMM : وهي إختصار لجملة Dual Inline Memory Module وتقوم بالنقل بشكل متوازي أي بتات بتان Bit 2 لذلك فهي أسرع من النوع الأول SIMM ، وتتكون من 168 Pin (دبوس) وسرعتها تصل من 100 إلى 133 MHz ، وظهرت في بدايات البينتيوم 2 .

ويمكن تمثيل شكلها بالرسم التالي :



3 – RIMM : وهي إختصار لجملة Random Inline Memory Module وهذا النوع ظهر مؤخراً أي في بداية البينتيوم 4 ويقوم بنقل الداتا وفقاً لحجمها أي أنها متغيرة وله نوعان :
3,1 – DDRAM : وهي إختصار لجملة Double Data Rate RAM وهذا النوع يتحمل سرعة من 200/266 MHz .

ويمكن تمثيل شكلها بالرسم التالي :



3,2 –RDRAM : وهي إختصار لجملة Random Data Rate RAM وهذا النوع يتحمل سرعة من 400/600 MHz وقد يصل إلى 800 .

ويمكن تمثيل شكلها بالرسم التالي :



أي أن الفرق بين النوعين السابقين هي السرعة فقط .

- ويوجد مشكلة في النوع RDRAM وهي أنه خرج في غير وقته أي أنه سبق أوانه فنحن نعرف أن اللوحة الأم Mother Board لها سرعة محددة مثلاً 400 وأحضرنا رام من هذا النوع سرعته 800 فهناك ضياع للكلفة والسرعة فقد ذهبت نصف كفائتها كرام يتحمل سرعة عالية وذلك بسبب أن اللوحة الأم لا تتحمل هذه السرعة.

- الذواكر الثابتة ROM :

- إختصار لجملة Read Only Memory أي ذاكرة للقراءة فقط وسميت كذلك لأننا لا نستطيع تعديل البيانات التي تحويها من حيث عمليات الإضافة أو الحذف أو التعديل ومكانه في اللوحة الأم .

- يطلق عليها أحيانا إسم BIOS وهي إختصار لمصطلح Basic Input Output System أي أن عمليات الإدخال والإخراج كلها تمر في هذه الوحدة وأيضاً تسمى CMOS .

- الرام يحتوي على لغة مشتركة بين جميع الأجهزة في عمليات الإدخال والإخراج مثل اللغة الإنجليزية فهي لغة موحدة Standard بين كل الشعوب ، وهي تحتوي على برنامجين أساسيين وهما :

1 - برنامج ال POST : إختصار لكلمة Power On Self Test ، ووظيفته تتضح من إسمه فأول كلمين هما Power On والتي تعني أنه هو الذي يوزع الكهرباء فنحن أول ما نقوم بالضغط على كبسة ال Power في الجهاز لفتحه يتولى هذا البرنامج إرسال الشرارة الأولى لل Power الذي بدوره يقوم بالتوزيع إلى مختلف أجزاء الحاسوب ، وهي مماثلة للسلف في السيارة فهو مسؤول عن تشغيل السيارة ككل . لذلك فهذا البرنامج مهم جداً ، وأي خلل فيه لا نستطيع العمل على الجهاز (لذلك فهو ثابت) . أما الجزء الثاني من الجملة فهي Self Test وهو يقوم بفحص جميع الأجهزة اللازمة لعملية إقلاع الجهاز أو تشغيله فهو يقوم بفحص الأجهزة التالية على التوالي :

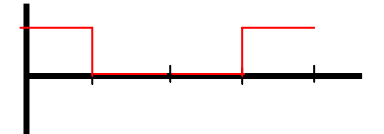
Mother Board → CPU → AGP → RAM → Keyboard .

فهو يقوم بإرسال Pulses للأجهزة وإستقبالها مرة أخرى فبذلك يعلم أن الجهاز موجود ومستعد . وأكبر مثال توضيحي على هذه العملية : عملية الرد على الهاتف حيث أننا إذا أردنا أن نتكلم مع شخص فنقول كلمة (ألو) لكي نعلم أن الطرف الآخر موجود . فإذا رد علينا فنعلم أنه موجود وإذا لم يرد علينا فنعلم أنه غائب أو أنه تخلى عن سماعة الهاتف .

2 – برنامج ال Boot Strap : وهو متخصص في إيجاد نظام التشغيل وتحميله Locate & Load وهو مسؤول عن إيجاء الأخطاء ومسكها لأنه هو الذي يتحكم بالأجهزة . وهو غالباً يقوم بتحميل الملفات الأساسية للنظام ووضعها في الرام ومن الملفات التي يقوم بتحميلها : Command.com وأيضاً Config.sys و Autoexec.bat وغيرها من الملفات التي تعمل على تبويت الجهاز .

- ذاكرة الكاش : سنشرح عنها بالكم الوافي عندما نصل إلى أجهزة الراوتر Router .

- يفهم الحاسوب المعلومات على شكل نبضات Pulses بواسطة الأرقام 1,0 على شكل 5V,0V على التوالي ، فمثلاً لو أننا أرسلنا 1001 فيقوم بإرسال 5 فولت ثم 0 ثم 0 ثم 5 . وتمثيلها بيانياً يتم بالشكل التالي :



حيث أن نبضة الواحد لأعلى ونبضة الصفر على مستوى الخط .

وأصغر وحدة في مقاييس الحاسوب هي البت Bit وتساوي خانة إما صفر أو واحد . ووحدة التعامل في الحاسوب تكون بالبايت Byte ويساوي 8Bit أي أنها تمثل خانة (حرف أو رقم ...) . وإليك وحدات القياسات في الحاسوب كلها :

Bit = 0 Or 1
Byte = 8 Bit
KB = 1024 Byte → Kilo Byte
MB = 1024 KB → Mega Byte
GB = 1024 MB → Giga Byte
TB = 1024 GB → Tera Byte
.....

- ولعل السؤال الأن لماذا 1024 وليس 1000 ؟؟؟

والجواب على ذلك لأننا نتعامل مع النظام الثنائي Binary System أي أن الأس هو 2 و لأن الكيلو 1000 أي أنها 10 مرفوعة للأس 10 فبالمثل للنظام الثنائي أي أنها 2 مرفوعة للأس 10 والتي تساوي 1024 .

التحويلات بين أنظمة العد المستخدمة في جهاز الحاسوب :

- يستخدم الحاسوب العديد من أنظمة العد المختلفة ومن أشهر أنظمة العد :

- النظام الثنائي Binary System : يستخدم الخانات 1,0 .
- النظام العشري Decimal System : يستخدم الخانات 1,2,3,4,5,6,7,8,9,0 .
- النظام الست عشري Hexadecimal . يستخدم الخانات 1,2,3,4,5,6,7,8,9,0,A,B,C,D,F .

وسنتحدث الأن عن التحويلات المختلفة بينها :
- التحويل من النظام الثنائي للعشري : Bin → Dec
هناك طرق عديدة للتحويل ولكني سأقوم بإدراج أسهل الطرق حرصاً مني على الفهم في التطبيق .
في هذه الطريقة التي سنستخدمها نقوم بكتابة مضاعفات الرقم 2 كالتالي :

... 128 64 32 16 8 4 2 1

ثم نقوم بكتابة الرقم الثنائي تحت الأرقام السابقة ولأننا لا نستخدم إلا 8 بتات فلا داعي لأكثر من 128 .
فمثلاً لو أخذنا الرقم 1 0 1 1 1 0 0 1 فنقوم بتحويله كالتالي :

128	64	32	16	8	4	2	1
1	0	0	1	1	1	0	1

ثم نقوم بجمع الأرقام التي تحتها 1 كما يلي :
1+4+8+16+128 ونحسب الناتج فيصبح : 157 إذن الرقم 1 0 1 1 1 0 0 1 بالعشري يساوي 157 .

لنأخذ مثالاً آخر : 0 1 0 1 0 0 1 1
نستخدم نفس الطريقة :

128	64	32	16	8	4	2	1
1	1	0	0	1	0	1	0

ثم نقوم بجمع الأرقام التي تحتها 1 كما يلي :
2+8+64+128 ونحسب الناتج فيصبح : 202 إذن الرقم 0 1 0 1 0 0 1 1 بالعشري يساوي 202 .

لنأخذ مثالاً آخر : 1 1 1 0 0 0 1 1
نستخدم نفس الطريقة :

128	64	32	16	8	4	2	1
1	1	0	0	0	1	1	1

ثم نقوم بجمع الأرقام التي تحتها 1 كما يلي :
1+2+4+64+128 ونحسب الناتج فيصبح : 199 إذن الرقم 1 1 1 0 0 0 1 1 بالعشري يساوي 199 .

- التحويل من النظام العشري للثنائي : Dec → Bin
هناك طرق عديدة للتحويل ولكني سأقوم بإدراج أسهل الطرق حرصاً مني على الفهم في التطبيق .
في هذه الطريقة التي سنستخدمها نقوم بطرح السؤال التالي (هل يوجد فيه ؟؟) أي أننا نقوم بالسؤال
هل يوجد في الرقم 128 أو 64 أو 32 .... فإذا كان الجواب نعم نقوم بوضح واحد تحت الرقم المطلوب

128	64	32	16	8	4	2	1
		X					

ثم نقوم بالطرح من العدد الكلي ... ونبقى نطرح إلى أن نصل إلى الرقم المطلوب وطبعاً بدون باقي
و كمثال على الكلام السابق إليك التالي :

نريد تحويل الرقم العشري 144 إلى النظام الثنائي !! فنقوم بعمل التالي :
!! هل الرقم 144 يحتوي على الرقم 128 !! – الجواب نعم . إذن نضع الرقم 1 تحت خانة ال 128 كالتالي :

128	64	32	16	8	4	2	1
1							

ثم نقوم بطرح 128 من العدد الكلي 144 فيصبح الناتج 16 .
ثم نقوم بطرح نفس السؤال !! هل الرقم 16 يحتوي على الرقم 64 !! فيكون الجواب لا إذن نقوم بوضح الرقم 0 تحت خانة الرقم 64 ونكرر ذلك على باقي الأعداد فيصبح الناتج :

128	64	32	16	8	4	2	1
1	0	0	1	0	0	0	0

وهذا مثال آخر :
نريد تحويل الرقم العشري 200 إلى النظام الثنائي !! فنقوم بعمل التالي :
!! هل الرقم 200 يحتوي على الرقم 128 !! – الجواب نعم . إذن نضع الرقم 1 تحت خانة ال 128 كالتالي :

128	64	32	16	8	4	2	1
1							

ثم نقوم بطرح 128 من العدد الكلي 200 فيصبح الناتج 72 .
ثم نقوم بطرح نفس السؤال !! هل الرقم 72 يحتوي على الرقم 64 !! فيكون الجواب نعم إذن نقوم بوضح الرقم 1 تحت خانة الرقم 64 ونكرر ذلك على باقي الأعداد فيصبح الناتج :

128	64	32	16	8	4	2	1
1	1	0	0	1	0	0	0

وهذا مثال آخر :

نريد تحويل الرقم العشري 255 إلى النظام الثنائي !! فنقوم بعمل التالي :
!! هل الرقم 255 يحتوي على الرقم 128 !! – الجواب نعم . إذن نضع الرقم 1 تحت خانة ال 128 كالتالي :

128	64	32	16	8	4	2	1
1							

ثم نقوم بطرح 128 من العدد الكلي 255 فيصبح الناتج 127 .
ثم نقوم بطرح نفس السؤال !! هل الرقم 127 يحتوي على الرقم 64 !! فيكون الجواب نعم إذن نقوم بوضح الرقم 1 تحت خانة الرقم 64 ونكرر ذلك على باقي الأعداد فيصبح الناتج :

128	64	32	16	8	4	2	1
1	1	1	1	1	1	1	1

أي أن الرقم 255 هو أعلى رقم يتحمله النظام الثنائي ذو الثمان خانات (بايت) .

- التحويل من النظام الثنائي للسادس عشر : Bin → Hex
هناك طرق عديدة للتحويل ولكني سأقوم بإدراج أسهل الطرق حرصاً مني على الفهم في التطبيق .
النظام السادس عشر هو نفس العشري ولكن هناك أرقام جديدة مضافة إليه ليحتوى على مجال أوسع فالحرف A يعني 10 بالعشري والحرف B يعني 11 بالعشري ... والحرف F يعني 15 بالعشري .
وطريقة تحويل الرقم من الثنائي للسادس عشر هي أسهل التحويلات وإليكم الطريقة :
نقوم بفصل الأرقام الثنائية من اليمين لليسار رباعيات أي أننا نقسم السلسلة كل 4 خانات . وإليك المثال التالي لتتمكن من فهم هذه العملية :
- لو نريد تحويل الرقم 01101011 الثنائي إلى النظام السادس عشر نقوم بالفصل كل 3 أحرف فتصحب كالتالي : 1011　0110 ونحولها كل مجموعة إلى ما يوازيها بالسادس عشر ..
فالقسم الأول هو عبارة عن 11 بالنظام العشري أي أنها تمثل الحرف B .
والقسم الثاني هو عبارة عن 6 في النظام العشري فنبقيها كما هي .
فيصبح الناتج　6B . وهكذا .....

- التحويل من النظام السادس عشر للثنائي : Hex → Bin
هناك طرق عديدة للتحويل ولكني سأقوم بإدراج أسهل الطرق حرصاً مني على الفهم في التطبيق .
هنا طريقة عكسية فأقوم أنا بأخذ الخانة وتحويلها لأربعة خانات باالثنائي فمثلاً 3 بالست عشري يساوي 3 بالعشري ويساوي 11 بالثنائي ولكا أقوم بوضع الأصفار فيصبح 0011 هذه الخانة الأولى .

مثال :
نريد تحويل D7 للنظام الثنائي :
نقوم بأخذ الرقم 7 وتحويله للنظام العشري أي 7 ثم نحوله للنظام الثنائي فيصبح 0111 (لاحظ أننا وضعنا الصفر هنا) ثم نأخذ الحرف D ونحوله للعشري فيصبح 13 أي 1101 . فيكون الناتج 11010111 .

مثال آخر :
نريد تحويل AB للنظام الثنائي :
نقوم بأخذ الحرف B وتحويله للنظام العشري أي 11 ثم نحوله للنظام الثنائي فيصبح 1011 ، ثم نأخذ الحرف A ونحوله للعشري فيصبح 10 أي 1010 . فيكون الناتج 10101011 .

- التحويل من النظام السادس عشر للعشري : Hex → Dec
هناك طرق عديدة للتحويل ولكني سأقوم بإدراج أسهل الطرق حرصاً مني على الفهم في التطبيق .
نقوم بأخذ الرقم ثم تحويله للثنائي ومن ثم للعشري .

مثال :
نريد تحويل الرقم F6 الست عشري للنظام العشري .
نقوم بالتحويل للثنائي فيكون الناتج : 11110110 ثم نحوله للعشري كالتالي :

128	64	32	16	8	4	2	1
1	1	1	1	0	1	1	0

نجمع التالي : 2 + 4 + 16 + 32 + 64 + 128 فيكون الناتج : 246 .

مثال آخر :
نريد تحويل الرقم DD الست عشري للنظام العشري .
نقوم بالتحويل للثنائي فيكون الناتج : 11011101 ثم نحوله للعشري كالتالي :

128	64	32	16	8	4	2	1
1	1	0	1	1	1	0	1

نجمع التالي : 1 + 4 + 8 + 16 + 64 + 128 فيكون الناتج : 221 .

مثال آخر :
نريد تحويل الرقم FF الست عشري للنظام العشري .
نقوم بالتحويل للثنائي فيكون الناتج : 1111111 ثم نحوله للعشري كالتالي :

128	64	32	16	8	4	2	1
1	1	1	1	1	1	1	1

نجمع التالي : 1 + 2 + 4 + 8 + 16+ 32 + 64 + 128 فيكون الناتج : 255 .

أي أن أقصى حد يتحمله العشري بالنسبة للبايت هو 255 .

- التحويل من النظام العشري للسادس عشر : Dec → Hex
هناك طرق عديدة للتحويل ولكني سأقوم بإدراج أسهل الطرق حرصاً مني على الفهم في التطبيق .
نقوم بأخذ الرقم ثم تحويله للثنائي ومن ثم للست عشري .

مثال :
نريد تحويل الرقم 213 العشري للست عشري .
نقوم بالتحويل للثنائي فيكون الناتج :

128	64	32	16	8	4	2	1
1	1	0	1	0	1	0	1

ثم نقسم الرقم الثنائي لقسمين أو أربعات فيكون الناتج 0101 للقسم الأول و 1101 للقسم الثاني فنأخذ القسم الأول ونحوله للست عشري فيصبح 5 ونقوم بأخذ النصف الثاني أيضاً فيكون D فيصبح الناتج الكلي : D5 بالنظام السادس عشر .

مثال آخر :
نريد تحويل الرقم 59 العشري للست عشري .
نقوم بالتحويل للثنائي فيكون الناتج :

128	64	32	16	8	4	2	1
0	0	1	1	1	0	1	1

ثم نقسم الرقم الثنائي لقسمين أو أربعات فيكون الناتج 1011 للقسم الأول و 0011 للقسم الثاني فنأخذ القسم الأول ونحوله للست عشري فيصبح B ونقوم بأخذ النصف الثاني أيضاً فيكون 3 فيصبح الناتج الكلي : 3B بالنظام السادس عشر .

مثال آخر :
نريد تحويل الرقم 255 العشري للست عشري .
نقوم بالتحويل للثنائي فيكون الناتج :

128	64	32	16	8	4	2	1
1	1	1	1	1	1	1	1

ثم نقسم الرقم الثنائي لقسمين أو أربعات فيكون الناتج 1111 للقسم الأول و 1111 للقسم الثاني فنأخذ القسم الأول ونحوله للست عشري فيصبح F ونقوم بأخذ النصف الثاني أيضاً فيكون F فيصبح الناتج الكلي : FF بالنظام السادس عشر .
أي أن أقصى حد يتحمله السادس عشر بالنسبة للبايت هو FF .

بسم الله الرحمن الرحيم

المحاضرة الثانية :
الإثنين 13-06-2005

مفهوم الشبكات Network :

هي عبارة عن مجموعة من الأجهزة ترتبط مع بعضها البعض عن طريق SWITCH OR HUBE أو راوتر Router حيث من خلالها يستطيع كل PC ان يتعرف على جميع ال PCs الاخرى الموجودة على نفس الشبكة .

وأي PC تستطيع تبادل المعلومات وإستخدام اي SW أو HW موجود على هذه الشبكه بشرط الصلاحيات .

– أجهزة الهارد وير Hardware :

وهي جميع الأدوات الخاصة لربط الشبكات ببعضها ، وتتكون من الأجهزة التالية :

1 – جهاز حاسوب PC : ومن منا لا يعلم جهاز الحاسوب الشخصي !! .

2 – إنترفيس Interface ويتكون من جهازين وهما : الموديم Modem و NIC .

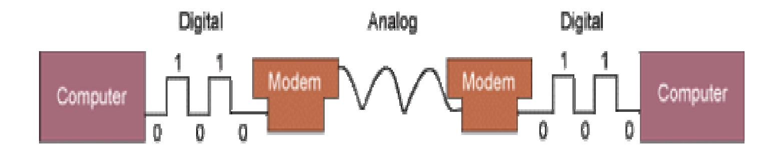
2.1 – جهاز الموديم Modem :

ويمكن توضيح وظيفته من إسمه فهو إختصار Modulation And Demodulation . وهذا الجهاز خاص للإتصال عبر الهاتف Dial-Up Connection ، وهو جهاز خاص لترجمة الإشارات الرقمية digital signals للإشارات النظرية analog signals والعكس بالعكس .

وتسمى عملية التحويل من الديجيتل إلى الأنالوج (Modulation) -- Modulation → DA .

وتسمى عملية التحويل من الأنالوج إلى الديجيتل (Demodulation) -- Demodulation → AD .

ويمكن توضيح العملية بالرسمة التالية :



وعملية التزويد بالإنترنت بالرسمة التالية :



ISP : مزود الإنترنت (مثال ذلك شركة WANADOO للإنترنت في الأردن) .

PSTN : شركة الإتصالات وذلك للتزويد بخدمة الإتصال الثابت (مثال ذلك شركة الإتصالات الأردنية) .

2.2 – كرت الشبكة NIC :
وهو إختصار لجملة Network Interface Card والمعروف بكرت الشبكة . وهو عبارة عن واجهة لشبكات اللان LAN .

ويحتوي هذا الكرت على ROM خاص به يخزن داخلها عنوان يسمى MAC Address وهو إختصار من جملة Media Access Control Address وهو عبارة عن عنوان للكرت Unique أي أنه لا يوجد منه إثنان في كل العالم وهو يتكون من 48 بت أي 48 رقم ثنائي مقسمان إلى جزئين متساووين ويمكن توضيح ذلك في الشكل التالي :

24	24
Organization Unique Identifier (OUI)	Specific Number

و 48 بت نحولها إلى الهيكسا يعني رباعيات (48/4) فينتج عندنا 12 خانة هيكسا (الست عشري) .

ولكي تعرف رقم الماك عندك يمكنك الذهاب :
- إذا كنت تمتلك NT/Me/200/Xp إذهب إلى Start ثم إنقر على Run وإكتب الأمر Cmd لكي يظهر لك ال Command Prompt ثم إكتب الأمر Ipconfig /all فيظهر الرقم بإسم Physical Address ويمكنك ملاحظة أنه يتكون من خانات Hex وليس Binary .
- إذا كنت تمتلك 98/95 إذهب إلى Start ثم إنقر على Run وإكتب الأمر Command لكي يظهر لك ال Command Prompt ثم إكتب الأمر Ipconfig /all فيظهر الرقم بإسم Physical Address ويمكنك ملاحظة أنه يتكون من خانات Hex وليس Binary .

وفكرة تقسيم عنوان الماك جائت من المنظمتان العالميتان IEEE وشركة ISO وهما منظمتان تمنحان الرقم الخاص الذي هو OUI (القسم على اليسار) أما القسم الذي على اليمين فتقوم الشركة التي تصنع الكروت بصناعته .

فمثلاً نفرض أن شركة A المتخصصة في صناعة كروت الشبكات NIC تريد أن تنتج رقم خاص بها فتذهب هذه الشركة إلى المنظمتان وتقوم بأخذ رقم خاص بالشركة A فتقوم الشركة بالتالي بإنتاج أرقام متسلسلة للقسم الأيمن كما تريد ولا يسمح لها بالعبث أو تغيير القسم الأ يسر .

3 – Media :
وهي عبارة عن الكوابل والأسلاك والوسائط المستخدمة في عمليات نقل وإستقبال المعلومات ، وتنقسم إلى ثلاثة أقسام حسب مادة النقل : ال Cables وال Fiber وال Wireless :

3.1 –ال Cables :
وفي هذا النوع يتم نقل البيانات إلكترونياً أي من خلال الإلكترونات ، وتقسم إلى نوعان رئيسيان : وهما ال Twisted وال Coaxial .

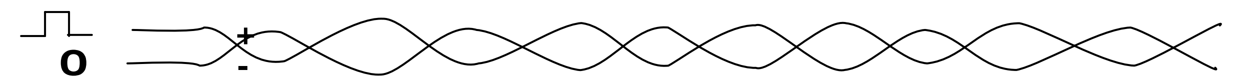
3.1.1 – كوابل ال Twisted :
- تقسم إلى قسمين UTP وال STP وهما متشابهان إلا أن النوع الاول هو المشهور لرخص ثمنه و مرونته و النوع الثاني مشابه للأول ولكنه محمي بطبقة عازلة من القصدير يحمية من المؤثرات الخارجية وهو غالي السعر لمناعته ضد أي أشعة مؤثرة على الأسلاك .
- ومدة نقل البيانات قبل تلاشيها هي تقريباً 100 m أي أن بعد هذه المسافة تذهب الإشارة نهائياً .
أما شكله فهو كما في الصورة التالي :
فلاحظ أنه يتكون من أربعة أزواج كل سلكين ملفوفين بشكل يظهرهما كأنهما سلك واحد .



أما القطعة التي تظم هذه الأسلاك فتسمى RJ-45
وهذه الصورة تدل عليها : (شكلها مستطيل شفاف)



والسؤال الآن : لماذا كل إثنين مترابطين ؟؟؟
والجواب كالتالي :
السلكان مقسومان لسلك يقوم بنقل البيانات والمعلومات وهو موجب
و السلك الآخر إسمه Ground أي أرضي وهو يحمل القيمة 0 - أي إشارة سالبة .
و تمثيله كما بالشكل التالي :



إذا حدث إن دخل إشعاع من الخارج سيتأثر السلكين بالعملية ويدخل نفس المقدار إلى السلكين كما في الشكل التالي :

الخط الموجب :

+5.7
خلل إشعاعي
بمقدار 0.7 V
+5
+5
+0
+0

الخط السالب Ground :

-0.7
خلل إشعاعي
بمقدار 0.7 V
-0
-0
-0
-0

بعد ذلك تأتي عملية المعالجة وذلك أنه في نهاية السلك المستخدم يأتي الجهاز المستخدم في عملية النقل ويستدعي Function خاصة تقوم بجمع الإشارتين وإخراج الناتج أي أنه يقوم بجمع إشارة السلك الموجب وإشارة السلك السالب .
كما بالشكل التالي :

+5-0
+5-0
+0-0
+5.7-0.7
+0-0

فيكون الناتج كما في الشكل التالي :

5
5
5
0
0

أي أن الإشارة هي 0110 ...

وتسمى العملية السابقة عملية الكنسلة Cancellation أي أن السلك أو الإشارة الخاطئة تقوم بإلغاء نفسها . وتسمى الأشعة أو عملية الخطأ بإسم إشارة Noise وهذه الإشارة تخرج من جميع الأجهزة التي نستعملها . فالجهاز يصدر هذه الإشارة والضوء (النيون) والتلفاز ..... وغيرها الكثير .
إذن علمنا الآن ما وظيفة السلك Ground والذي غالباً ما يكون بنفس لون السلك الموجب ولكنه يحتوي على خط أبيض .

3.1.2 – كوابل ال Coaxial :
تشبه هذه الكبلات كبل التلفزيون المعروف وتأتي بأشكال مختلفة والأكثر شهرة هي المستخدمة مع الشبكات بنوعيها الثخينة (Thick) و الرفيعة (Thin) .

- Thin coaxial : عرضه 0.5 و يمكن أن تحمل الإشارة إلى 185 ثم يبدأ الإشارة بالتلاشي تدريجياً .
- Thick coaxial : عرضه 0.7 و يمكن أن تحمل الإشارة إلى 500 ثم يبدأ الإشارة بالتلاشي تدريجياً .

ويمكنك التعرف إليه من خلال صورة :



وأيضاً من خلال الموصل T Connector المستخدم لربط الأجهزة ببعضها .



حيث يتم توصيل ممر للجهاز وممر لباقي الشبكة .

3.2 – الفايبر Fiber :
وسط لنقل المعلومات و الداتا من خلال الضوء ..
فالضوء أسرع بكثير من الإلكترونات ، وهو باهظ الثمن خصوصاً للشبكات الصغيرة ويحتوي على عديد من الميزات أهمها :

- مجال النقل كبير جداً .
- سريع جداً ويمكن أن تصل السرعة إلى 2-1 جيجا بايت في المسافات القصيرة .
- سلامة الإشارة من ال Noise الكهربائي
- السرية العالية إذا لا يستطيع أحد أن يخطف الإشارة .

ويمكنك رؤية صورته .

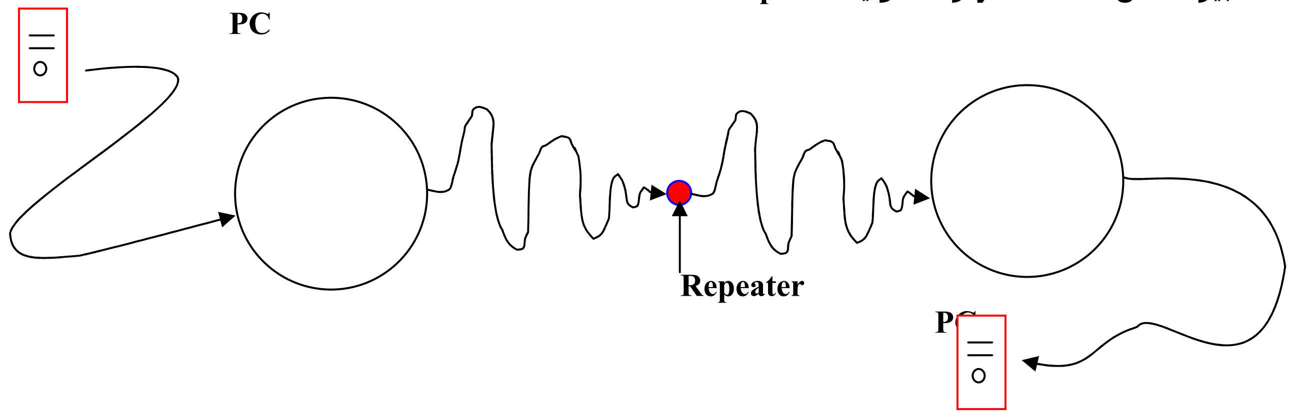


وديناميكية عمله : أنه يقوم بإرسال الإشارة الضوئية حسب زاوية معينة يقوم الطرف الآخر بإلتقاطها : والمادة ممكن أن تكون من الزجاج أو من البلاستيك للمرونة . وينقسم إلى نوعين :

- إشارة فردية Single Mode : وتنقل إشارة واحدة في الوقت ومداه 3 KM .
- إشارة متعددة Multi Mode : وتنقل إشارات متعددة في الوقت ومداه 2 KM .

3.3 – اللاسلكي Wireless :
ومعنى ذلك إستخدام الإشارات اللاسلكية (بدون أسلاك) .. ولنا فيه كلام كثير في درس الراوتر .

4 – المكرر Repeater :
نحن نعلم أنه بعد المسافة التي يسمح بها كل نوع من الأنواع المختلفة من الوسائط (Media) تضعف الإشارة وتتلاشى تدريجياً إلى أن تختفي . لذلك كان لا بد من مقوي ومضخم للإشارة خصوصاً للمسافات الكبيرة فمن هنا جاء جهاز المقوي Repeater .



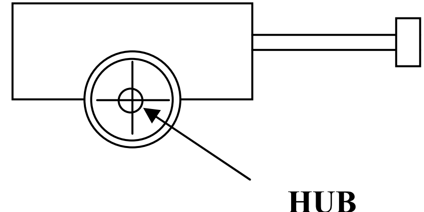
وله وظيفتان أساسيتان وهما :
- تضخيم الإشارة Amplifier .
- إعادة الإرسال Resend .

وهو عبارة عن موصل أحادي أي أنه يستقبل وصلة واحدة ويرسل وصلة واحدة .

فإذا كان عندنا شبكة طويلة ونريد أن نستخدم شبكة LAN خلالها فنقوم بوضع أجهزة ريبيتر بين الفترة والأخرى ولكن يجب علينا مراعاة قاعدة (3 – 4 – 5) في المحاضرة الرابعة .

وبالرغم من أن المكررات تستطيع زيادة حجم الشبكة إلا إنها لا تستطيع أن تستمر أكثر من حجم البناية الداخلية لها .

5 – جهاز ال HUB :
لو قمت بكتابة كلمة Hub في أي قاموس لوجدت أن معناها العجلة ...
هل شاهدت في عمرك عربة ؟؟؟ كما في الشكل !!!



الدبوس الموجود في وسط العجلة إسمه Hub .

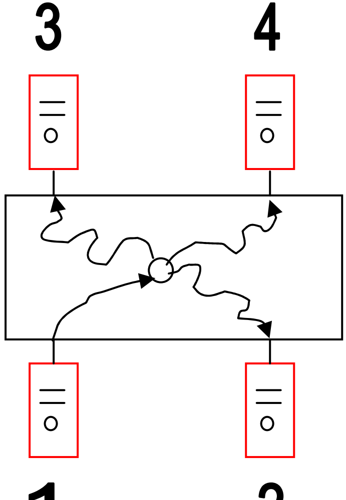
أي أنها تعني الرابطة أو نقطة التركيز . وهذه هي مهمتها :
نفس مهمة المكرر ولكنها نقطة إنتشار فهي تستقبل وصلة وترسل أكثر من وصلة . 1 To Many .

وجهاز ال Hub ناتج من فكرة الشبكة ذو الشكل النجمي فيكون ال Hub في مركز الشبكة لوصل العقد مع بعضها ويتم وصل كل جهاز PC مع ال Hub بحيث يقوم ال Hub باستخدام هذا التوصيل لإرسال الإشارات إلى كافة العقد الموصولة معه وكافة الأجهزة PC's .

ومهامه نفس المكرر :
- تضخيم الإشارة Amplifier .
- إعادة الإرسال Resend بطريقة الإنتشار Propagation .

- وهناك سيئة وهي : أن جهاز ال Hub واحد يرسل فقط والأجهزة الأخرى كلها مستقبلة . يعني لا يجوز أن يرسل جهازين في الوقت الواحد ... وهذه سيئة قاتلة ...

وطريقة الإنتشار :
يقوم بإرسال المعلومة لجميع الأجهزة PC's الموجودة على الشبكة وليس من مهمتها أن تعرف أن المعلومة قد تم إيصالها أم أنها إنقطعت ، المهم أنه يقوم بالإرسال .



كمثال : لو أننا نريد إرسال معلومة من جهاز 1 إلى جهاز 2 فالآلية التي تقوم عليها هذه الطريقة كما في الرسمة التالية :

أي أنها ترسل المعلومة إلى جميع الأجهزة ومن خلال الجهاز المستلم يحدد أنها له أم لا .
المهم أنه يستقبل المعلومة .

وهذه أكبر مشكلة للجهاز (طبعاً الجهاز إنقرض) .

وهذه المشكلة تستهلك وقت و سعة Bandwidth
لأنها تعالج في ال CPU (السؤال هل المعلومة لي أم لا) .

ومن هنا يمكننا تعريف أنماط الإرسال :

- طرق الإرسال Transmission :

1 – أحادية العمل Simplex :
في هذه الطريقة يكون هناك طرفين إحداهما يستقبل فقط
ولا يرسل والآخر يرسل فقط ولا يستقبل لهذا إسمه أحادي الإتجاه . →

2 – مزدوجية العمل Half Duplex :
وهنا يقوم جهاز واحد بالإرسال في الوقت الواحد ويقوم الجهاز الآخر بالإستقبال ومن ثم يمكن الجهاز الآخر أن يرسل ولكن بشرط أن يستقبل الطرف الآخر . بمعنى أنه واحد يرسل وواحد يستقبل ولا يهم من هو الطرف . → OR ←
ومثال ذلك : أجهزة الشرطة فيقوم شخص بالتكلم ثم يقول كلمة " حوّل " ليقوم الطرف الآخر بالإنتقال من دور المستقبل إلى دور المرسل ، وكمثال آخر أجهزة وطريقة الإتصال لشركة Express الأردنية .

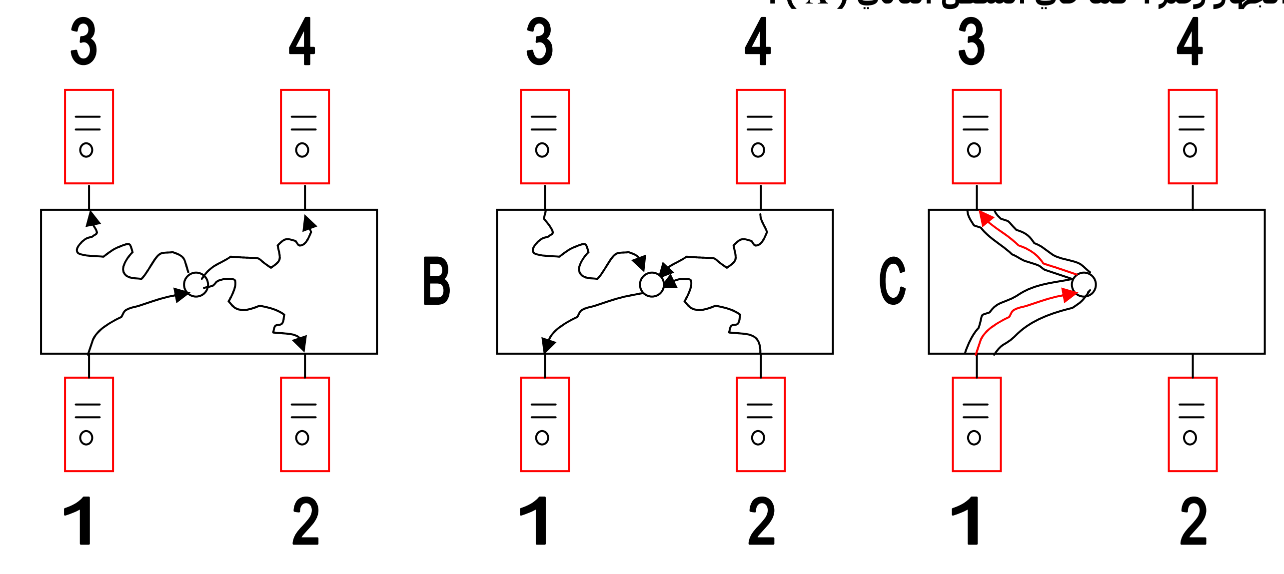
3 – ذو الطرفين Full Duplex :
وهنا يمكن للجهازين أن يستقبل أو يرسل في نفس الوقت . ↔
ومثال ذلك أي شركة إتصال عادية .

- وجهازي ال Repeater وال Hub يستعملات الطريقة 2 وهي Half Duplex .

6 – جهاز السويتش Switch :
يشبه المحول بالشكل الخارجي ولكنه يعد أفضل في تسريع أداء الشبكة وذلك لانه يستطيع الاحتفاظ بجدول عناوين العقد التي يتصل بها وعندما تصل إليه إشارة من عقدة ما يرسل هذه الإشارة إلى الهدف المقصود فقط وهو عكس ما كان يقوم به ال HUB إذ كان يرسل الإشارة إلى كل العقد بدون إستثناء .
طريقة ومبدأ النقل في السويتش يختلف إختلافاً تام عن ال Hub بمعنى أن السويتش أفضل من ال Hub بألف مرة والسبب في ذلك طريقته :
قبل أن يرسل الرسالة يقوم أولاً بطلب الماك للأجهزة
نسمي هذه العملية (Mac Request) فيرسل رسالة طلب
وكل الأجهزة التي تسمعه أو تستطيع الرد عليه تقوم بإعطاءه الماك للجهاز PC فيقوم بعد ذلك بالتخزين وبمنطقة ال Buffer جدول يضم إسم المعبر Port ورقم الماك الخاص بالجهاز .
فينتج عندنا جدول كما في الشكل التالي :

Port	MAC
1	MAC A
9	MAC B
11	MAC C
….	……

ولو إفترضنا وجود 4 أجهزة ويريد الجهاز رقم 1 أن يرسل رسالة إلى الجهاز رقم 4 كما في الشكل التالي (A) :



بعد إرسال طلب ال MAC Request يتم إستلام جميع الماك لجميع الأجهزة PC كما في الشكل (B) .

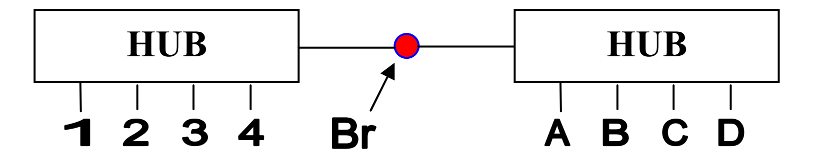
ثم يقوم السويتش بفتح معبر Port خاص لهذه العملية (C) ويقوم بالإرسال ومن ثم إغلاق هذا المعبر .
إذن نستطيع إدراج ميزاته كما يلي :

- وظائفه هي : التضخيم Amplifier ويعمل على مبدأ Full Duplex .
- درجة الأمان عالية فيه .
- يستطيع إرسال أو إستقبال أكثر من مرة في الوقت الواحد ففي مثالنا السابق يستطيع الجهاز رقم 2 أن يرسل للجهاز رقم 3 . وهكذا ...
- السويتش مسؤول عن فتح المنفذ Port وعن إغلاقه .
- سرعة النقل تصل إلى 100 mbps أي ما يقارب 10 أضعاف سرعة النقل لل HUB .

7 – الجسور Bridge :
نفس مبدأ وطريقة السويتش إلا أنه أحادي الإتجاه أي ذو مدخل واحد للإستقبال وذو مخرج واحد للإرسال ، وغالباً يستعمل للربط بين أجهزة الشبكة مثل ال HUB أو ال Switch ...

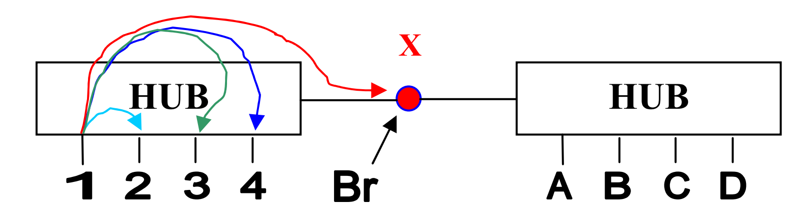
و العمل الرئيسي الذي يقوم به الجسر هو الربط بين شبكتين مختلفتين في التركيب الداخلي ، مثل : ربط شبكة Ethernet مع شبكة Token Ring حتى لو كانت الشبكتان تستخدمان بروتوكولات مختلفة ، ويقوم بحفظ جدول به كل العناوين الفيزيائية MAC Address للعقد ويسمى هذا الجدول جدول ال ARP وهو إختصار للجملة Address Resolution Protocol وهو يقوم بمراقبة الشبكة و حركة المرور وعند إستلامة لإشارة ما يقوم بفحص جدول ال ARP فإذا كانت العقدة الهدف داخل الشبكة الفرعية ، لا يسمح للإشارة بالخروج ، و إذا كانت في شبكة فرعية آخرى سمح لها بالخروج . وكتوضيح أكثر للعملية الأخيرة يمكننا تفسيرها بواسطة الرسم كالتالي :

لنفترض أنه يوجد عندنا جهازي HUB كما في الشكل :



ونريد أن نرسل معلومة من الجهاز 1 إلى الجهاز 4 ، فلو إفترضنا أنه لا يوجد عندي جسر هنا فسيقوم ال HUB بإرسال رسالة إلى جميع الأجهزة من على اليمين وجميع الأجهزة من على اليسار ، وهنا كارثة فلو إفترضنا أني أمتلك شبكة بواقع 1000 جهاز ، فماذا تتوقع أن يحدث !!! (الجواب عندك)

فيقوم ال HUB بإرسال المعلومة لجميع الأجهزة في الطرف الأيسر كما في الشكل التالي :



ولكن !!! قبل إرسالها للجزء الأيمن يقوم الجسر بطلب جميع الماك للأجهزة على الطرف الأيمن ثم ينظر هل الماك المطلوب إيصال المعلومة إليه موجود عندي !!!! إذا كان الجواب نعم يقوم بفتح منفذ ... (كما في السويتش) ، أما إذا كان الجواب لا فيقوم بعمل Disconnection لعملية النقل (على الطرف الأيمن) . أو أنه يقوم بالنظر هل الماك عندي من الشبكة اللتي على اليسار إذا كان الجواب نعم فلا يسمح لها بالمرور . وهذا المبدأ مستخدم أيضاً في السويتش .

- إذا كانا الجهازين الموصولين بالجسر متوافقين في السرعة نسميهما Symmetric .
- إذا كانا الجهازين الموصولين بالجسر غير متوافقين في السرعة نسميهما Asymmetric .

- يمكننا الأن تعريف معى كلمة Broadcast : وهي طريقة عمل السويتش والجسور ومعناها أن كل البيانات المنتقلة خلال هذين الجهازين تنتقل من خلال قرارات وليس (هيك عباطة) .
- ونستنتج أيضاً أن جهازي السويتش والجسور تعتبر أجهزة ذكية على خلاف جهاز ال HUB .
* كل الأجهزة السابقة من 1 إلى 7 تعد أجهزة شبكة ال LAN . أي أنها شبكات محدودة .

8 – جهاز الراوتر Router :
وهو أول جهاز يربط بين شبكات ال WAN وال LAN بكفاءة . وهو أفضل جهاز من الأجهزة السابقة على الإطلاق بسبب مزايا كثيرة سنذكرها لاحقاً . ويمكن أن نقول أن الراوتر هو جهاز PC كامل .

وهو يقوم بعمل مهم جدا في الشبكات ذات الفروع المتعددة إذ إنه يقوم بإرسال الإشارات من شبكة إلى آخرى حتى لو كانت هذه الشبكات موصولة بعدد من الشبكات الفرعية ، وتستخدم الراوترات جدول ARP مثل جدول الجسور والسويتشات و يتميز عنهما بعدة أمور منها .. يعتمد جدول ال ARP في الراوتر على عناوين الشبكات مثل أرقام ال IP الخاصة لكل PC و به خارطه لأقصر وأسرع مسار بين الفروع و الأجهزة الآخرى و المسافات الفاصلة بينها .

*** ستكون ثلاثة أرباع المحاضرات التالية عن الراوتر وكيف نعمل له Configuration لأنه هو الذي يهمنا في عمليات الشبكات ، فهو مستخدم على نطاق عالمي .

- أنواع الشبكات حسب المنطقة :
يمكن أن نقسم الشبكات إلى أقسام حسب المنطقة الفاصلة كالتالي :

1 – الشبكة المحلية LAN :
وهي إختصار من جملة Local Area Network ، وهي شبكة ذو منطقة محدودة وأكبر مسافة لها 100 m أي أنها لا تتعدى البناية بحالها .

2 – الشبكة المحلية الممتدة MAN :
وهي إختصار من جملة Metropolitan Area Network ، ويمكن أن نقول أن الحرف M إختصار لكلمة Medium ، وهي شبكة ذو منطقة أكبر من شبكة ال LAN ، وأكبر مسافة لها مدينة بأكملها .

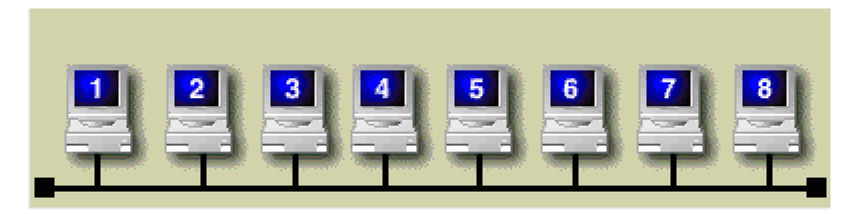
3 – الشبكة الممتدة WAN :
وهي إختصار من جملة Wide Area Network ، وهي شبكة ذو مساحة غير محددة (أي مفتوحة) .

4 – الشبكة التخزينية SAN :
وهي إختصار من جملة Storage Area Network ، و هي أي شبكة من الشبكات السابقة ولكن التخزين لا يكون على الجهاز PC ، بل يكون على سيرفر خاص بهذه العملية ، وكل العمليات على البيانات من حذف وتعديل وإضافة تتم على السيرفر .

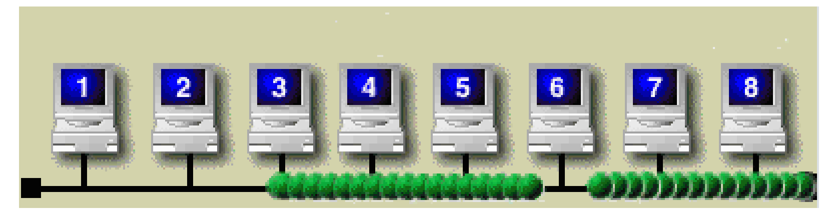
5 – الشبكة المحلية اللاسلكية WLAN :
وهي إختصار من جملة Wireless Local Area Network ، شبكة محلية ولكنها من غير أسلاك يعني عبر الأمواج اللاسلكية .

- أنواع الشبكات حسب الشكل Network Topology :
يمكن أن نقسم الشبكات إلى أقسام حسب شكل الشبكة كالتالي :

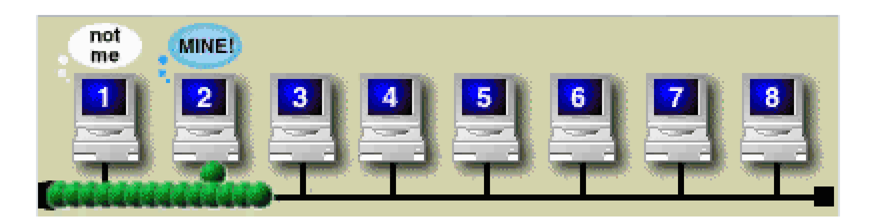
1 – الإستراتيجية المستقيمة BUS Strategy :



وهذه الإستراتيجية تحتوي على فلسفتين للعمل إحداها نظري Logical و الأخرى عملي Physical :
Physical : أما عن الناحية العملية فيقصد بها الشكل العام للإستراتيجية ، فنلاحظ هنا أنها تحتوي على أسلاك مربوطة ب T-Connector ، وعلى جانبي الشبكة يوجد مسد للمعبر Terminator .
Logical : الناحية النظرية وهي أنه من خلال الجهاز المرسل ، ترسل إشارة تسمى ال Media على شكل نبضات إلكترونية يتم إستقبالها من جميع الأجهزة كما في الشكل التالي :

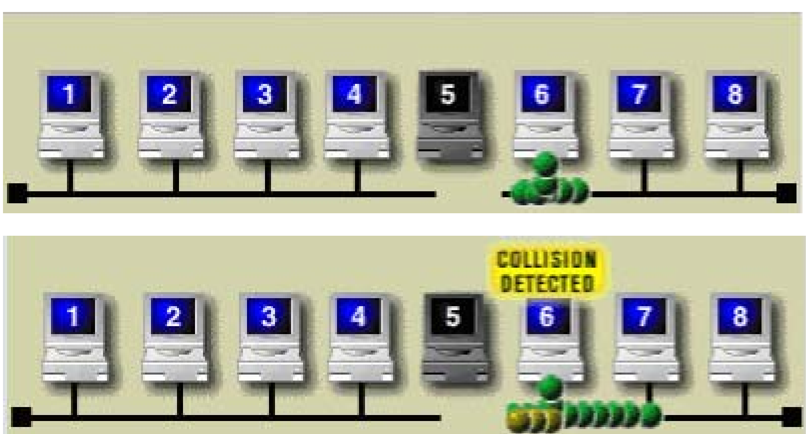


ومن ثم تقوم بسؤال الأجهزة الأخرى :: هل هذه المعلومة لك ؟؟ ويقوم الجهاز بردها إذا كانت ليست له وقبولها إذا كانت له كما في الشكل :



وعندما تصل إلى النهاية تتلاشى الإشارة .
و تفصيل عملية أخذ المعلومة من المرسل إلى المستقبل كالتالي :
يقوم الجهاز المرسل بإرسال ال Media لكل جهاز فتقوم هذه الإشارة بالمرور تدريجياً من أول جهاز إلى آخر جهاز وتسأل هل هذه المعلومة لك يا جهاز ؟؟ فإذا كان الجواب لا ينتقل إلى غيره ليبحث عن الجهاز الهدف ، أما إذا كان الجواب نعم يقول للجهاز المستقبل إنتظر قليلاً ريثما أقوم بتحميل الداتا ويستمر بالقول للأجهزة الأخرى : ممنوع الإستقبال أو الإرسال لأنه يوجد عندي جهاز يريد الإستقبال ، فيذهب مرة أخرى ويأتي بالمعلومة من الجهاز المرسل ثم يعطيها للجهاز المستقبل .

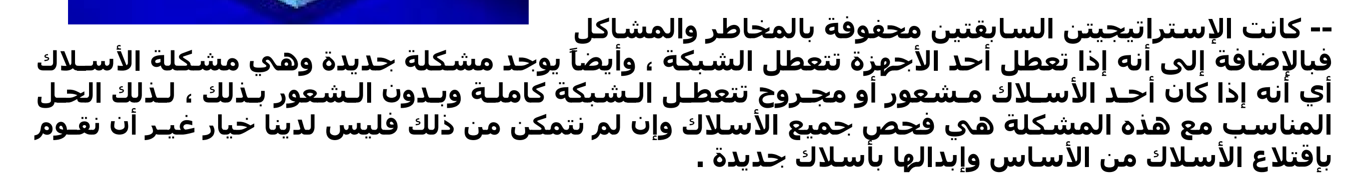
ومن أكبر مشاكل هذه الطريقة أنه إذا حدث وأن تعطل أحد الأجهزة ، كل الشبكة تتعطل كما في الشكل التالي :



2 – الإستراتيجية الحلقية Ring Strategy :

تشبه إلى حد كبير الشكل BUS ولكنها من غير Terminator على الأطراف أي أن الطرف الأيمن موصول مع الطرف الأيسر .
ولكن هنا قمنا بإنشاء خط آخر بحيث أنه إذا إنقطع الخط الأول نستطيع أن نرسل البيانات عبر الخط الثاني ...

وتحتوي على نفس مشكلة الشكل BUS وهي أنه إذا كان أحد الأجهزة معطل تتعطل الشبكة كاملة .



-- كانت الإستراتيجيتين السابقتين محفوفة بالمخاطر والمشاكل فبالإضافة إلى أنه إذا تعطل أحد الأجهزة تتعطل الشبكة ، وأيضاً يوجد مشكلة جديدة وهي مشكلة الأسلاك أي أنه إذا كان أحد الأسلاك مشعور أو مجروح تتعطل الشبكة كاملة وبدون الشعور بذلك ، لذلك الحل المناسب مع هذه المشكلة هي فحص جميع الأسلاك وإن لم نتمكن من ذلك فليس لدينا خيار غير أن نقوم بإقتلاع الأسلاك من الأساس وإبدالها بأسلاك جديدة .

3 – الإستراتيجية النجمية Star Strategy :
هي عبارة عن إستراتيجية مركزية ففي الوسط نقوم بوضع جهاز إما Hub أو Switch أو Router أو أي أجهزة من أجهزة الشبكات . ونوصله مع الأجهزة الأخرى ، ومن أهم ميزات هذه الطريقة أنه إذا تعطل أحد الأجهزة لا تتعطل الشبكة أبداً . هذا بالنسبة للناحية العملية Physical .

أما ال Logical : بطريقتين :
1 - CSMA :
إختصار ل Carrier Sense Multiple Access
القسم الأول : Carrier Sense
في كل مرة يريد جهاز أن يرسل معلومات يقوم بتحسس الميديا هل هي مشغولة (تنقل بيانات أخرى) أم هي فارغة و متاحة !! فإذا كانت فارغة يقوم بنقل الداتا من وإلى الأجهزة المطلوبة ، أما إذا كام مشغول فيقوم بالإنتظار Randomly أي بفترة زمنية عشوائية .
القسم الثاني : Multiple Access
أي أنه يستطيع أن يرسل أكثر من مرة في وقت واحد .

2 – CD/CA :
CD إختصار من Collision Detection وهي إكتشاف أنه يوجد عندي حالة تعارض ، ويكون حل هذه المشكلة بإيقاف الجهازين المرسل والمستقبل وإعادة الإرسال . (تكون بعد عملية الإرسال)
CA إختصار من Collision Avoidance وهي منع حدوث التصادم قبل عملية الإرسال أو أثناء .

4 – الإستراتيجية الهرمية النجمية Hieratical Star Strategy :
و هي عبارة عن مجموعات Star مربوطة مع بعضها بشكل هرمي .
5 – الإستراتيجية الهجينة Hybrid Strategy :
وهي هجين من الأنواع السابقة فمثلاً شبكة تحتوي على Bus و Star في نفس الوقت .
6 – الإستراتيجية الشبكية Mesh Strategy :
في هذه النوعية يكون كل جهاز مرتبط مع كل جهاز بالشبكة ، فمثلاً لو أني أمتلك أربع أجهزة فإني أربط الجهاز الأول مع الأجهزة الأخرى والجهاز الثاني مع الأجهزة الأخرى والجهاز الثالث مع الأجهزة الأخرى والجهاز الرابع مع الأجهزة الأخرى . وهكذا ... لاحظ أنها غير عملية ومكلفة فهي تحتاج العديد من الأسلاك ولكنها تؤمن منع إنقطاع الشبكة ، فمن خلال أي جهاز تستطيع الوصول لجهاز آخر .

بسم الله الرحمن الرحيم

المحاضرة الثالثة :
الأربعاء 15-06-2005

طريقة النقل عبر الشبكات :

يقوم مبدأ النقل على النظام المسمى بـ OSI وهو إختصار لجملة Open System Interconnection وهي تكنولوجيا مستخدمة في عمليات النقل وموحّدة على مستوى العالم .
وتتكون هذه الإستراتيجية من 7 طبقات Layer وهي :

7 – طبقة نوع التطبيق المستخدم Application Layer .
6 – طبقة نسق الملف Presentation .
5 – طبقة ال Session .
4 – طبقة النقل Transport .
3 – طبقة ال Network .
2 – طبقة ال Data Link .
1 – طبقة النقل الفعلي Physical .

- يمكن التعبير عنها بالجملة التالية لسهولة الحفظ : All People Seen To Need Data Processing .

- فإذا خرجت المعلومة من ال PC المصدر Source إلى ال PC الهدف Destination يتم تطبيق الطبقات من الطبقة رقم 7 نزولاً إلى الطبقة رقم 1 . (ما يحدث في الجهاز المصدر)
- و إذا أتت المعلومة إلى ال PC الهدف Destination من ال PC المصدر Source يتم تطبيق الطبقات من الطبقة رقم 1 صعوداً إلى الطبقة رقم 7 . (ما يحدث في الجهاز الهدف)

وهنا شرح لجميع الطبقات بالترتيب من الطبقة السابعة إلى الطبقة الأولى :

7 – طبقة نوع التطبيق المستخدم Application Layer :
في هذه الطبقة ، و عندما يقوم المستخدم User بعملية الإرسال ، يتم تخزين ومعرفة البرنامج المستخدم في صناعة الملف المرسل ، وهو بالتالي البرنامج الذي سيستعمله الملف لعملية الفتح في الجهاز المستقبل ، فلو أخذنا على سبيل المثال الملف (Test.txt) فنعلم أن البرنامج المستعمل هو Notepad .

6 – طبقة نسق الملف Presentation :
في هذه الطبقة يتم تخزين النسق Format للملف المرسل ، فعندما نرسل ملف txt.* مستحيل أن يفتح على برنامج Windows Media Player كأنه ملف avi.* ، بل يقوم بفتح برنامج ال Notepad بنفس النسق الذي أتى به ، وإذا كان الملف مضغوط Compression أو مشفر Encryption يتم تحليله في هذه الطبقة .

5 – طبقة ال Session :
يمكن أن نسمي هذه الطبقة بوزير الخارجية فهي المسؤولة عن التنسيق مع نفس الطبقة في الجهازين المستقبل والمرسل ، فهي المسؤولة عن فتح القناة وإدارتها وفصلها أثناء عمليات النقل ، وهي المسؤولة عن المعلومات Information الملف المرسل و حالته هل وصل أم لا ، وكيفية إيصاله .

4 – طبقة النقل Transport :
وظيفة هذه الطبقة تقسيم الملف إلى أجزاء صغيرة تسمى Segment ، وتتمركز أهميته في تقسيم الملف إذا حدث وإنقطع الخط فلا نضطر للإرسال من البداية ، بل نقوم بعملية إسترجاع Error Recovery للأجزاء التالفة ، و الأجزاء التي سلمت تبقى في الجهاز المستقبل .
و لنأخذ الخزانة مثالاً على ذلك ، فلو أننا نريد أن ننقلها خارج غرفة ما وكان حجم الباب صغير ، فلا نستطيع نقلها لكبر حجمها (Bandwidth) لذلك نقوم بتجزيئها ونقل كل جزء على حدى ... وإن حدث أن كسر جزء نقوم بتصليحه على إنفراد أو الإتيان بجزء جديد من غير الإضطرار إلى شراء خزانة كاملة جديدة .

و حجم الأجزاء يتم الإتفاق عليها في طبقة ال Session ، ويتم الإتفاق أيضاً على طريقة الإرسال هل هي متزامنه Synchronous أي مفصولة بفترات زمنية أم غير متزامنه Asynchronous أي متتالية ؟؟

3 – طبقة ال Network :
في هذه الطبقة يتم إضافة قسمين للجزء Segment ، وهما عنوانا ال IP الخاص للجهازين المرسل والمستقبل ، وذلك للتأكيد على معرفة الجهازين المعنيين بعملية النقل .

Des. IP	Source IP	Segment

وتسمى هذه الطبقة Header L 3 أي المستوى الثالث .
و الوحدة المؤلفة من ال Segment بالإضافة لـ S. IP أي العنوان للجهاز المرسل و ال D. IP للجهاز المستقبل تسمى بـ Packet .

2 – طبقة ال Data Link :
في هذه الطبقة يتم إضافة قسمين آخرين لل Packet ، وهما عنوانا الماك للجهازين المرسل والمستقبل MAC Address وسنتحدث عنه بالتفصيل في محاضرة لاحقة . أيضاً يتم إضافة قسمين في مؤخرة ال Packet وهما ال FCS وال CRC . كالتالي :

Des. Mac	S. Mac	Des. IP	Source IP	Segment	CRC	FCS

وتسمى هذه الوحدة كاملة بالإسم Frame وأيضاً تسمى هذه الطبقة بالإسم Header L 2 أي المستوى الثاني .

ولكن !!! لماذا قمنا بإضافة عنوان الماك MAC Address ؟؟
الجواب : في الطبقة السابقة أي الطبقة رقم 3 يقوم جهاز الراوتر بإستعمال عنوان ال IP فقط ، وذلك للمرونة في عمليات تبادل الملفات ، ويستطيع أيضاً التعامل مع العنوان ال MAC ... لكن جهازا السويتش وال Hub لا تستطيعان التعامل إلا مع عنوان ال MAC ..

ولكن !!! ماذا يحدث لو تخلينا عن ال IP بما أن الراوتر يستطيع التعامل بواسطة عنوان ال MAC ؟؟
والجواب : هي أننا لو قمنا بإزالة ال IP فلن نستطيع المرور من خلال الطبقة الثالثة ... لذلك لن يكون عندي عملية نقل أبداً .

- إختصار CRC من الجملة التالية Cyclic Redundancy Check وهي خوارزمية Algorithm تستخدم للكشف عن الأخطاء For Error Detection ، فهي تقوم بالإتفاق مع طبقة ال Session في الجهازين على رقم عشوائي ، ثم يقوم الجهاز المصدر Source PC بقسمة ال Data على الرقم العشوائي ويقوم بالإحتفاظ بناتج القسمة ، ثم يقوم بإرسال ال Data إلى الجهاز الهدف Destination PC ، وهناك أيضاً نقوم بتقسيم ال Data المستقبلة على نفس الرقم العشوائي ومقارنة ناتج القسمة بين الجهازين . فإذا كانا متساويين تكون ال Data المرسلة صحيحة وعملية النقل صحيحة . أما غير ذلك فيكون هناك خطأ بنسبة 100% في عملية نقل ال Data .

ولنأخذ مثالاً على هذه العملية : فعندنا معلومات مرسلة ولتكن 01011011 ولنتفق على رقم عشوائي وليكن 101 لنستخدمه في عملية التقسيم ، قمنا بالإتفاق عليه من كلا طبقتي ال Session في الجهازين المرسل والمستقبل ، ولنفترض أن المعلومة وصلت إلى الجهاز المستقبل كالتالي : 01011001 . نقوم الآن بالتأكد بواسطة الخوارزمية CRC . فنقوم بعملية القسمة كالتالي :

```
01011011          01011001
101      /        101      /
--------          --------
10010             10001
```

فنلاحظ أن الناتج
إذن ::: يوجد خلل .

وهذه وظيفة خوارزمية CRC ، إكتشاف الأخطاء .

- إختصار FCS من الجملة التالية Frame Check Sequence ووظيفة هذه الخوارزمية ترقيم ال Segment إلى أرقام حسب ترتيبهم في الملف ، فإذا حدث أن إنتقلت Segment قبل الأخرى ، يتم الترتيب في الجهاز المستقبل حسب الخوارزمية FCS .

1 – طبقة النقل الفعلي Physical :
تقوم هذه الطبقة بتحويل ال Frame إلى أرقام ثنائية 1,0 ومن ثم تحميلها على ال Media .

-- بعد الطبقة الأولى يتم نقل المعلومة كاملة من الجهاز المرسل إلى الجهاز المستقبل ...
- وبالنسبة للإستلام من جهاز المستقبل Des. PC يتم التعامل مع ال Data من الطبقة 1 إلى 7 تراجعي .

- وهذه الطبقات غير موجودة فعلياً أي أنها نظريات قمنا بشرحها لنفهم كيفة نقل المعلومة من جهاز لآخر .

وبالنسبة للأجهزة يمكن تصنيفها كالتالي بالنسبة للطبقات :
حيث أن العلاقة هرمية ، فالمستوى الثالث يستطيع التعامل مع المستوى الثاني والأول ، لكن المستوى الأول لا يستطيع التعامل مع المستوى الثاني ولا المستوى الأول ...

3 – Network	Router (IP)
2 – Data link	Switch / Bridge / NIC (MAC)
1 – Physical	HUB / Repeater / Media

نلاحظ في الجدول السابق ، أن الراوتر يستطيع التعامل مع الطبقة الثالثة بواسطة ال IP لأنه يحتوى على وظائف كثيرة تأهله لعمل ذلك ، إذن نستطيع القول أن جهاز الراوتر أفضل جهاز في القائمة .
وأيضاً الأجهزة : ال Switch وال HUB و ال NIC ، يستطيعون التعامل فقط مع ال MAC Address .

إستدعاء الجهاز بإسمه دون عنوانه بواسطة ال DNS :
إختصار ال DNS قادم من جملة Domain Name Service أي خدمة إسم الدومين ، وهو موجود في طبقة ال Application ، وهو المسؤول عن إستدعاء جهاز بواسطة إسمه دون الحاجة لل IP ، فنحن نعلم أنه بإمكاننا الدخول لجهاز عبر الشبكة دون الحاجة لمعرفة عنوانه IP . ولكن كيف ؟؟؟

يقوم ال DNS بتخزين أسماء الأجهزة المتوافرة على الشبكة وعنوانها بجدول يقوم بتخزينه في الكاش أي الذاكرة العشوائية ، فعندما نقوم بإستدعاء جهاز بالإسم ، يقوم ال DNS بتحويل الإسم إلى عنوان IP ثم يقوم بالبحث عنه في الجدول الخاص به فإذا كان موجود تمّت العملية بنجاح ، أما إن لم يكن موجود فتظهر لك رسالة تنبهك إلى أن الإسم غير موجود ...!!!

- وهنا معلومة مهمة لا يدريها كثير من مستخدمي الإنترنت ، فهل لاحظت يوماً أنك عندما تقوم بكتابة عنوان بريد الياهو www.Yahoo.com ما يحدث في الشريط السفلي المسمى بشريط الحالة ؟؟
أكيد قمت بذلك ، فهو يقوم بكتابة عبارة تدل على أنه يقوم بالبحث عن عنوان ال IP الخاص بسيرفرات الياهو ... من خلال إسمه في جدول الكاش للسيرفر الذي تستخدمه ، ولو أنك قمت بكتابة ال IP الخاص بالسيرفر !! لفَتحت صفحة الياهو بشكل أسرع لأنك تقوم بإضاعة وقت وذلك بالبحث عن عنوان الياهو .
أي أننا في الطبقة الثالثة نقوم بإرسال ال Media لإحضار جميع ال IP الخاصة بالموقع المطلوب .

جدول ال ARP :
وهو إختصار لجملة Address Resolution Protocol ، ومعناها الحصول على عنوان ال MAC من خلال عنوان ال IP . و يقوم ببناء جدول يضعه عنده في الكاش .

بروتوكول ال TCP / IP :
ظهر هذا البروتوكول الخاص أو هذه الهيكلية من خلال وزارة الدفاع الأمريكية ، وذلك لإنشاء بروتوكول خاص بهم ، وقاموا بإعادة هيكلة للطبقات حيث جعلوها بأربع طبقات بدلاً من سبع طبقات كالتالي:

Application
Presentation
Session
Transport
Network
Data Link
Physical

OSI Model

Application
Transport
Internet
Network Interface

TCP/IP Model

- أما عن ماهية ال TCP / IP : فهي عبارة عن بروتوكول نقل Transport (TCP) وبروتوكول للشبكة Network Layer أي (IP) .ويمكن توضيح البروتوكولات لكل طبقة كالتالي :

Application Layer

DNS | FTP | HTTP | RIP | SNMP | SMTP | Telnet

Transport Layer

TCP | UDP

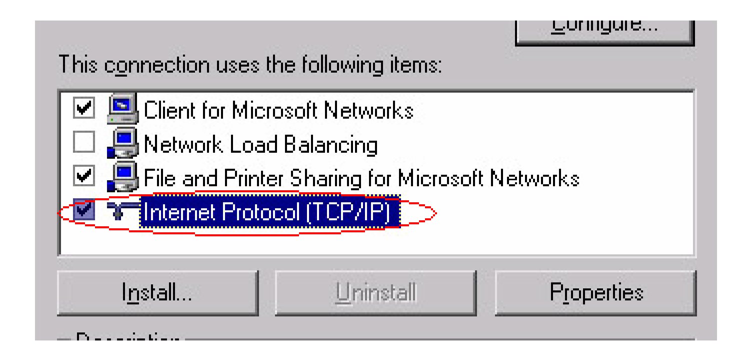
Internet Layer

IP | ARP | ICMP | IGMP | IPSEC

Network Interface Layer

Ethernet | Token Ring | FDDI | X.25 | Frame Relay

وهذه الصورة توضح جميع الموديولز لكل طبقات ال TCP / IP .
ولمعرفة أين يمكن تعريفه وضبطه في جهازك إليك هذه الصورة المؤلوفة :



البروتوكولات المسؤولة عن عمليات النقل في طبقة ال Transport Layer :

داخل طبقة ال Transport يوجد بروتوكولان لعمليات النقل وهما : TCP و ال UDP .

برتوكول ال TCP : وهو إختصار لجملة Transport Control Protocol ووظيفته السيطرة على عملية الإرسال ، وهو أيضاً مسؤول عن عملية نقل ال Data من خلال المستخدم End User .

بروتوكول ال UDP : وهو إختصار لجملة User Data Protocol وهـذا البروتوكـول خـاص بـال PC فهـي لغـة التخاطب بينها ، ويتم من خلاله الإتفاق على عمليات النقل ومتطلباتها .

- خصائص بروتوكول ال TCP :
يوجد خصائص لهذا البروتوكول وهي :
1 – 3 Way Hand Check :
في هذه العملية يقوم ال PCs المعنيان بعملية النقل على الإتفاق على زمــن محـدد للرد (الإستلام) إن تم إرسـال ال Data أم لا ، وإذا حدث أن لم ترسل ال Data يقوم المستقبل بالإنتظار ثلاثة أضعاف المدة المتفق عليها ، وإذا لم تصله يقوم بطلبها مرة ثانية . كما في الشكل الجانبي :

Segment 1
Acknowledge 2
Segment 2 X
Acknowledge Segment 2
Segment 2

وسميت بالتشبيك الثلاثي لأنها تحتوي على ثلاث عمليات وهي أخذ ثم طلب ثم أخــذ . كما في الشـكل التالــي :

Segment 1
Acknowledge 2
Segment 2

2 – الموثوقية والصحة Real able :
لأنه في حال لم ترسل بيانات (كما في الحالة الأولى) يقوم بالسؤال عنها ، ويبقى يـسأل عنهـا إلـى أن تصله ، فهو موثوق ولا يمكن أن تضيع بيانات أبداً من خلاله .

3 – عمليات الفتح والإغلاق Connection – Oriented .
لأنه هو المسؤول عن فتح قناة إتصال Connection عند الإرسال ، وهو أيضاً المسؤول عـن إغلاقهـا ، ويجب عليه إرسال البيانات إلى الطرف الآخر .

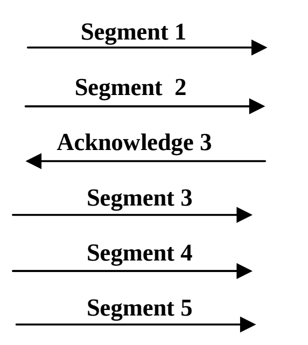
- خصائص بروتوكول ال UDP :
يوجد خصائص لهذا البروتوكول وهي :
1 –2 Way Hand Check :
وهي تقوم بالأخذ فقط دون الطلب . كما في الشكل التالي :
ويجب علينا أن نذكر هنا أن عمليات النقل أسرع بكثير من ال TCP لأنها تحتاج عمليتان فقط وليس ثلاث .

Segment 1
Segment 2

2 – غير موثوق به Unreal able :
لأنه إن حدث وأن لم ترسل بيانات (كما في الحالة الأولى) لا يقوم بالـسؤال عنهـا ، فهـو غيـر موثـوق ويمكن أن تضيع بيانات من خلاله .

3 –Connection – Less .
ليس له علاقة بفتح ال Connection أو إغلاقها .

- البروتوكولان السـابقان قد يكونا معروفين بالنسبة لك إن ذكرنا الإســم المـرادف لهمـا فـي عمليـات النقـل ، فـالبروتوكول TCP يـستخدم ال FTP لعمليـات النقل وهـو إختـصار مـن File Transport Protocol أي أنـه البروتوكول المسؤول عن نقل البيانات ، أما البروتوكول UDP فيستعمل ال TFTP وهو غالبـاً مـستخدم فـي عمليتا التنزيل Download (للسرعة) .



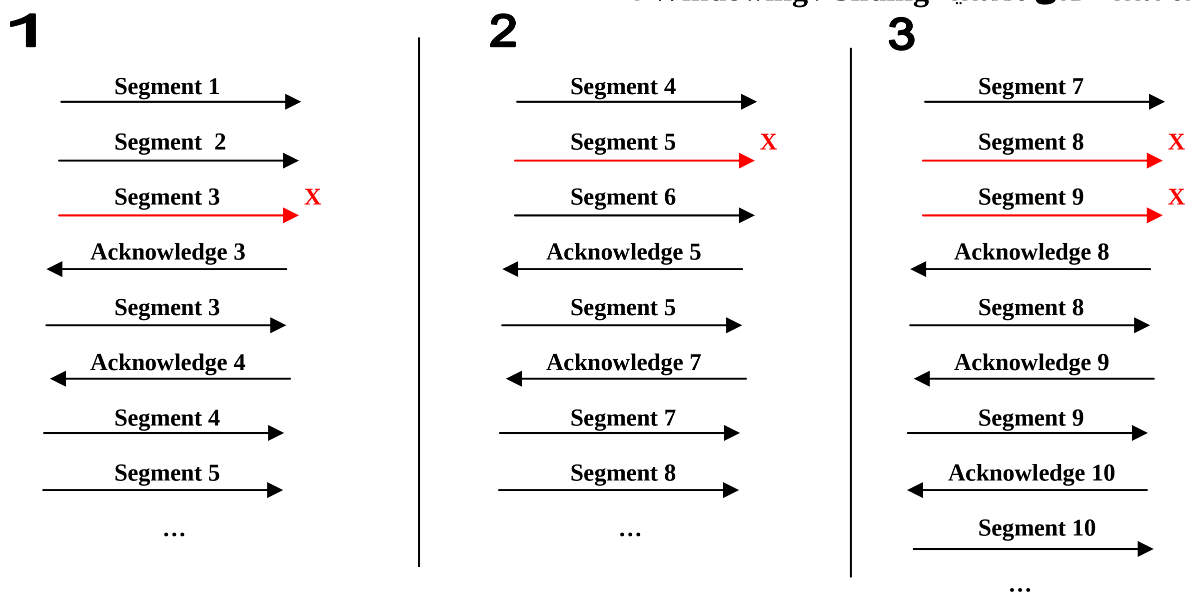
ولكي نقوم بزيادة كفاءة وسرعة البروتوكول FTP المسؤول عن عمليات النقل ، صمم هذا البروتوكول ليتحكم بنفـسه ، أي أنه يقوم بزيادة عـدد ال Segment المرسـلة في الوقت الواحـد ، وهذا ما يعرف بالمصـطلح Windowing / Sliding وهــي عمليات الزيــادة والنقــصان فـي عــدد ال Segment المرسلة في الوقت الواحد ، ويمكننا تمثيل هذه العــملية بالشكل التالي :
أي أننا إذا وجدنا أن الخط يتحمّل ويمكـــننا زيادة عدد ال Segment نقوم بذلك تدريجياً ، ولكن إن كثرت الأخطاء وقام بطلب Segment بشكل كبير نقوم بالتقليل إلى أن يستقر الخط . والعمــلية مســتمرة ، أي أننا نقوم

مرّة بالزيادة ومرة أخرى بالتقليل وسميت بإسم Sliding / Windowing لتشابه العملية ، فنحن على سبيل المثال نقوم بفتح الشبابيك إذا وجدنا أنه لا يوجد غبار خارجاً ، وكلما إشتدت الريح أو زادت الغبار نقوم بإغلاق الشبابيك تدريجاً . وهذه الفكرة جاءت لزيادة الأداء Performance والكفاءة .

وعمليات الزيادة والنقصان تناقش من الطرفين أي من ال Source وال Destination ، والعدد الإفتراضي المتفق عليه هو 1 في عمليات النقل وأيضاً إن حدث Error Correction يكون معدل النقل 1 أيضاً ، أي نقل واحد وطلب واحد (متتالي) .

وهذه العملية تجري وأنت لا تدري !! . فهل قمت بتنزيل ملف ولاحظت أنه يقوم بزيادة المعدل مرة ويقوم بالتقليل مرة أخرى !!! هذه هي العملية وهذا سببها (أضفها لمعلوماتك) .

وهذه أمثلة على العملية Sliding / Windowing :



في المثال رقم 1 :
قمنا بإرسال Segment 3 ، وحدث خطأ بالقطعة الأخيرة لذلك قمنا بالسؤال عنها مرّة أخرى وأرسلناها ثم طلبنا ال Segment رقم 4 ولم نقم بالإرسال إلا مرة واحدة لأننا قلنا أنه في حالة ال Error Correction لا نرسل إلا واحدة فقط ، فأرسلناها واحدة وطلبنا واحدة فقط .

في المثال رقم 2 :
قمنا بإرسال Segment 3 ، وحدث خطأ بالقطعة الثانية لذلك قمنا بالسؤال عنها مرّة أخرى وأرسلناها ثم طلبنا ال Segment رقم 5 ولم نقم بالإرسال إلا مرة واحدة لأننا قلنا أنه في حالة ال Error Correction لا نرسل إلا واحدة فقط ، فحدث عندي خلل في القطعة رقم 5 ثم أرسلناها وطلبنا القطعة رقم 7 لأن القطعة رقم 6 وصلت سالمة عندي ، وكما الحال في المثال الأول أرسلنا الخامسة ثم طلبا واحدة فقط (وليس أكثر من واحدة) .

في المثال رقم 3 :
قمنا بإرسال Segment 3 ، وحدث خطأ بالقطعة الثانية والثالثة لذلك قمنا بالسؤال عن الأولى مرّة أخرى وأرسلناها ثم طلبنا ال Segment الثانية التي حصل فيها خلل وهي رقم 9 ، وكما الحال في المثال الأول أرسلنا ثم طلبا واحدة فقط (وليس أكثر من واحدة) .

وهنا نكون قد أنهينا المحاضرة الثالثة بنجاح ... وأرجوا أن تكون قد إستفدت من هذه المعلومات ، وأن تعلم أن عملية نقل أو تنزيل ملف ليست بالأمر السهل بالنسبة لل PC .

بسم الله الرحمن الرحيم

المحاضرة الرابعة :
السبت 19-06-2005

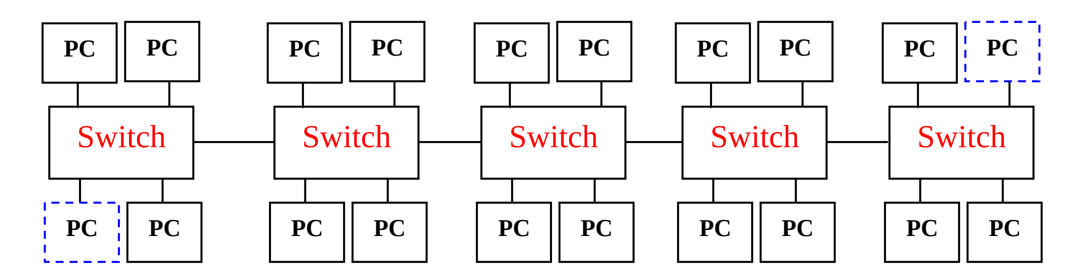
تركيب الشبكة المحلية LAN Installation :

عندما نقوم بتركيب شبكة داخلية محلية LAN يجب علينا مراعاة قاعدة 3 – 4 – 5 وكثير من المستخدمين لا يراعونها أو قد لا يعرفونها أصلاً ، وإليك بيان كل شيء :

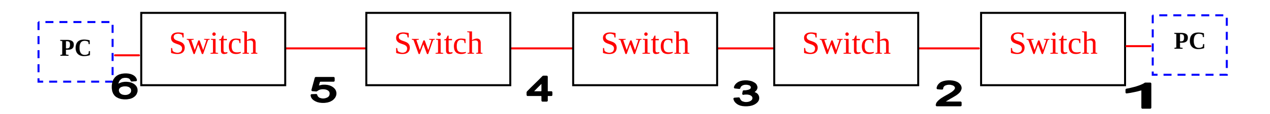
5 : Segment Maximum
4 : LAN Device Maximum
3 : Used Segment

5 : إذا زاد عدد الوصلات بين الجهازين عن خمسة ، لا يتم نقل بيانات أبداً .
4 : إذا زاد عدد الأجهزة المستخدمة في عملية النقل عن أربعة ، لا يتم نقل بيانات أبداً .
3 : إذا زاد عدد الوصلات المستخدمة في عملية النقل عن ثلاثة ، لا يتم نقل بيانات أبداً .

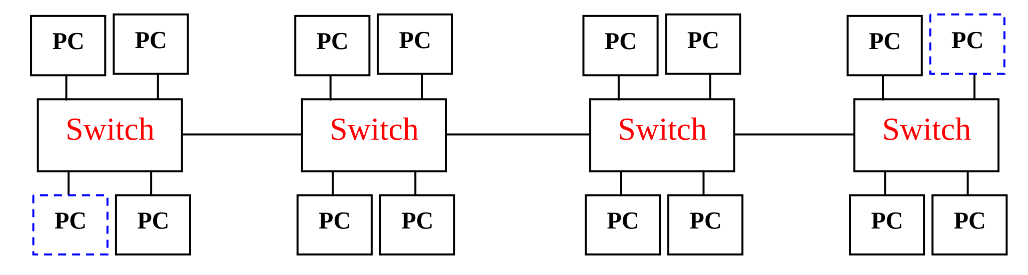
القاعدة 5 :
نقوم بأخذ الجهاز الأول في الشبكة المعنية ثم نقوم بأخذ الجهاز الثانية و نضعهم على شكل مستقيم (نظرياً وليس عملياً) ونقوم بحساب الوصلات الكلي بينهما ، وقد تكون الوصلات بين الأجهزة PC ، أو الأجهزة المستخدمة في عمليات النقل مثل ال Switch ... إلخ ، وهذا مثال على ذلك :



نريد نقل البيانات بين الجهازين باللون الأزرق ، نقوم بأخذ الجهازين على إنفراد وإيجاد عدد الوصلات المستعملة لعملية النقل ، كالتالي :

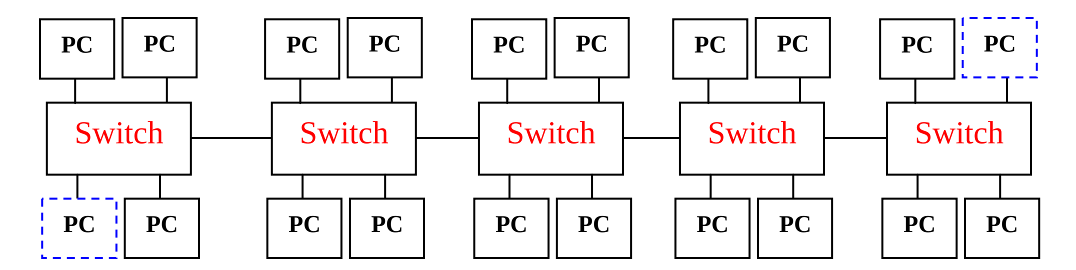


نلاحظ هنا أن عدد الوصلات المستعملة هي 6 وهي أكثر من العدد 5 ، إذن لن يرى الجهازين بعضهما في نفس الشبكة لأنه تم حدوث خلل في القاعدة 5 ، وهذه مشكلة Technical لا ينتبه لها معظم المستخدمين للشبكات أو الواضعين للشبكة المحلية .
وهذا مثال صحيح على القاعدة :



فهنا عدد الوصلات خمسة ...

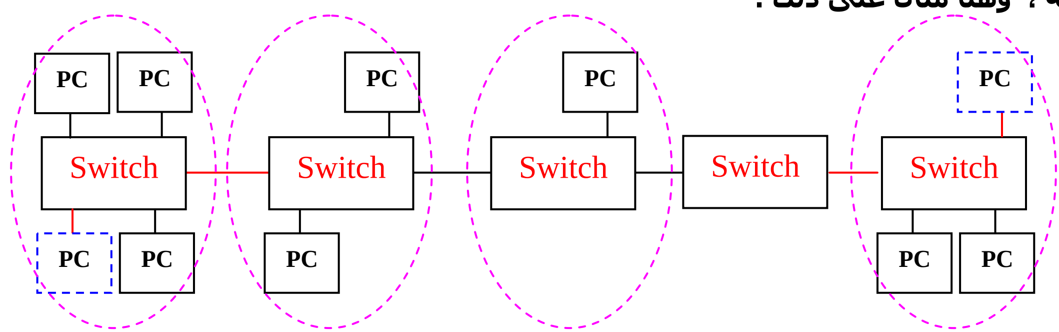
القاعدة 4 :
إذا زاد عدد الأجهزة (فقط أجهزة التوصيل) مثل السويتش والراوتر وغيرها عن أربعة ، دون النظر إلى الأجهزة PC ، فإننا نقول أن الجهازين لا يرون بعضهم ، ولنأخذ مثالاً على ذلك :



فهنا عدد الأجهزة 5 وهي أكبر من العدد 4 ، إذن يوجد خلل .

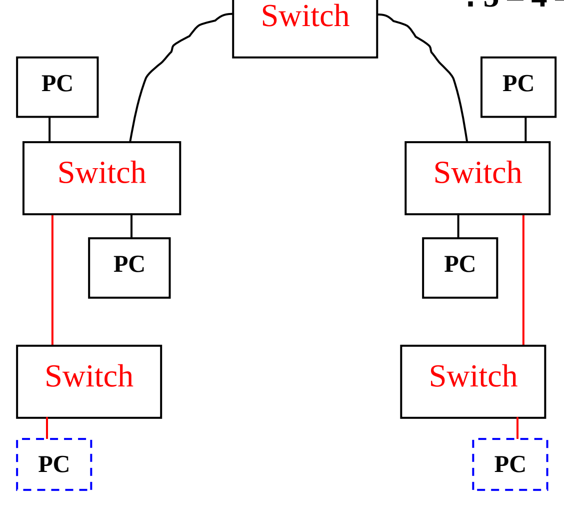
القاعدة 3 :

إذا زاد عدد الوصلات المستعملة عن ثلاثة (وهنا أي وصلة كان جهاز ال PC طرف فيها نسميها مستعملة) ، فنقول أن الجهازين لا يرون بعضهم في الشبكة . وكل جهاز شبكة مرتبط مع أجهزة PC نعتبره وصلة مستعملة ، وهنا مثال على ذلك :



فلاحظ معي أن عدد الوصلات المستخدمة 4 أي أنها مخالفة للقاعدة 3 .

لنأخذ مثالاً على شبكة ونطبق عليها القاعدة 3 – 4 – 5 :

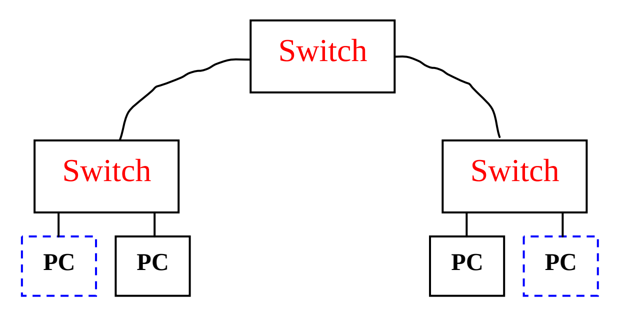


أولاً :
عدد الوصلات الكلي 6 ،
فشلت قاعدة ال 5 .

ثانياً :
عدد الأجهزة الكلي 5 ،
فشلت قاعدة ال 4 .

ثالثاً :
عدد الوصلات المستعملة 4 ،
فشلت قاعدة ال 3 .

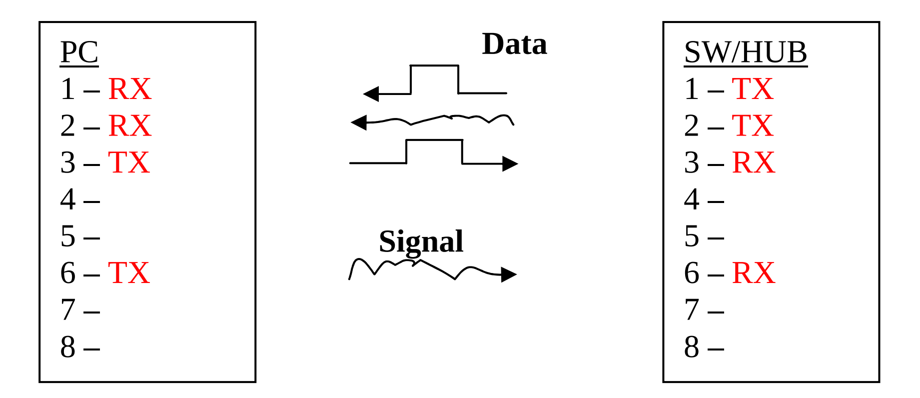
لذلك ، نستخدم الشكل الهرمي ، بدلاً من الشكل المستقيم .كما في الشكل التالي :



ففي الشكل التالي :
عدد الوصلات الكلي تساوي 4
عدد الأجهزة المستخدمة 3
وعدد الوصلات المستعملة 2

* أما في حالة الشبكات الكبيرة فنستخدم أجهزة الراوتر بدلاً من هذه الشبكة الصغيرة .

طريقة شبك الأجهزة بواسطة الأسلاك :
تتكون أجهزة الإتصالات بالشبكة بما فيها ال PC من مخارج لربطها مع بعضها ، وهي تتكون من 8 Pin ، و الشكل التالي لتركيبة أجهزة ال NIC وأجهزة ال Switch وال HUB :



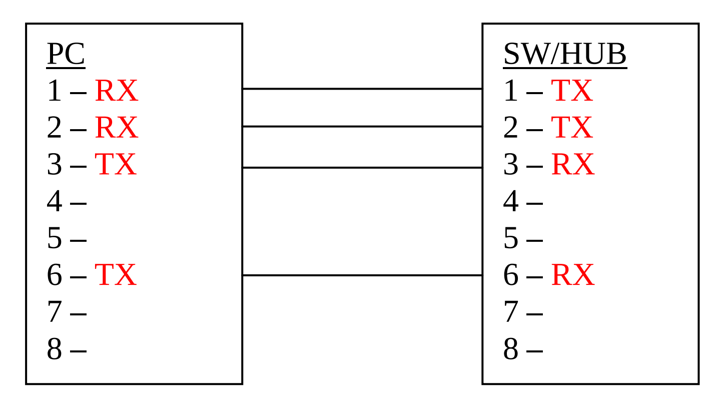
يتكون المخرج في ال PC من 8 أسلاك يوجد إثنان فقط للإرسال و إثنان الإستقبال . حيث :
TX : للإرسال Transport .
RX : للإستقبال Receive .

ولاحظ معي أن كل مخرج للإرسال يجب أن يتصل مع مخرج للإستقبال ، فلا يجوز أن يكون المخرجان مستقبلان أو مرسلان ، أي بمعنى أنه يجب أن يكونا مختلفين .

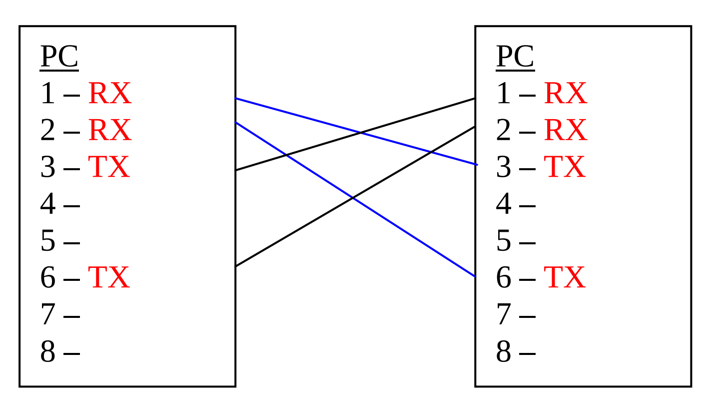
طرق التوصيل وصناعة الكوابل :
بين الأجهزة المختلفة نستخدم كوابل ال UTP وقد شرحناها من قبل ، وهناك ثلاث طرق لصناعة كيبل حسب الأجهزة المستعملة في الأطراف ، كالتالي :

1 – طريقة ال String Through :
وهي تستعمل للربط بين :
PC → SW
PC → HUB
Router → SW
Router → HUB

وسميت بهذا الإسم لشكلها المستقيم

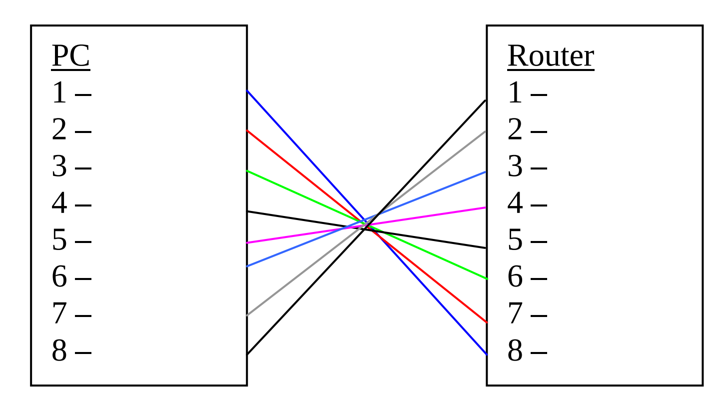


2 – طريقة ال Cross-Over :
وهي تستخدم للربط بين جهازين متشابهين :
PC → PC
HUB → HUB
SW → SW
SW → HUB
لأن جهازي ال SW وال HUB تعتبر أجهزة متساوية أي جهاز واحد .
وسميت بذلك لشكلها المتقاطع .



3 – طريقة ال Roll-Over :
وهذه الطريقة حصرياً للربط بين ال PC وال Router وذلك لعمل Configuration له ، وذلك من منفذ ال Console .

وهنا تستعمل وصلة خاصة تسمى DB male 9 وهي تتكون من طرفان طرف بالسيريال (COM) والطرف الآخر هو UTP .



ترتيب الألوان في كوابل ال UTP :

هناك ترتيبان عالميان ، وهما EIA / TIA 568A و EIA / TIA 568B والإسـمين EIA و TIA هما منظمتـان عالميتان مسؤولتان عن تنظيم الألوان في هذه الكوابل .

وإليك الآن ترتيب كل نوع على حدى :

EIA / TIA 568B	EIA / TIA 568A
1 – White Orange	1 – White Green
2 – Orange	2 – Green
3 – White Green	3 – White Orange
4 – Blue	4 – Blue
5 – White Blue	5 – White Blue
6 – Green	6 – Orange
7 – White Brown	7 – White Brown
8 – Brown	8 – Brown

والنوع EIA / TIA 568B هو الأكثر إنتشاراً .
وكل نوع من النوعان السابقان له إختلافات في الإستعمال حسب الأطراف المستخدمة .

بسم الله الرحمن الرحيم

المحاضرة الخامسة :
الأربعاء 22-06-2005

ماهية بروتوكول الشبكة IP وأقسامه :

يتكون ال IP من 32 Bit ، ويقسم إلى أربعة أقسام ، ويمكن تسميته 4 Octets أي أربع مجموعات ثمانية لأنه يقسم إلى ثمان بتات لكل قسم كالتالي :

______8Bit______ ،	______8Bit______ ،	______8Bit______ ،	______8Bit______
Oct	Oct	Oct	Oct

وهو قابل للتغيير Logical خلاف ال MAC Address الذي يعد Physical والذي لا يمكن تعديله أبداً .
ويطلق مصطلح Identity على عنوانا ال IP وال MAC لجهاز ما ، فهو المعرّف لجهاز ما .

ومن أهم وظائف ال IP أنه هو الذي يحدد هل الجهاز الذي يحمله في نطاق شبكة ما أم لا ، و يقسم فعلياً إلى قسمين وهما :
Network Part (NP) : و هو القسم الأيسر ، ويجب أن يكون متشابه لنفس الشبكة .
Host Part (HP) : وهو القسم الأيمن ، وهو يختلف لكل جهاز بالشبكة .

ونضرب مثالاً لتفهم طبيعة كلا الجزئين :
لو قمنا بأخذ ثلاثة شبكات خلوية في بلد ما (الأردن مثلاً) : فاست لينك ، و موبايل كوم ، وشبكة أمنية ومفاتيحها : 079 ، 077 ، 078 على التوالي . وقمنا بأخذ أرقام عشوائية لهواتف خلوية كالتالي :

NET	HOST
079	652842
077	245256
079	652421
078	552458
077	254415
078	852546

فهنا يمكن معرفة ال NP وال HP بكل سهولة ، فال NP هو الرقم أو العنوان الذي يضم أكثر من جهاز في شبكة واحدة ، وهنا نرى أن الأرقام التي على اليسار (المفاتيح) هي قسم الشبكة Network Part ، ويمكن أيضاً تمييز كل الأرقام التي في نفس الشبكة بمساواة القسم الأيسر مع الأرقام وأخذ المتشابه .

أما ال HP فنلاحظ أنها مختلفة تماماً ولا يمكن معرفة الشبكات التي ينضم إليها ، و لا يجوز أن يتساوى رقمين بهذا القسم .

تقسيمات وأنواع ال IP :

هناك تقسيمات وأنواع لل NP وال HP . وهي مصنفة حسب العدد المطلوب للشبكة المختارة ، أي أنه إذا كان العدد قليل أو متوسط أو كبير يمكننا إختيار النوع الملائم لذلك ، فلا يصح أن أنشأ شبكة تستوعب 1000 عنوان ، لـ 15 جهاز !! ، وإليك التقسيمات :

Class A : -------NP------- , -------HP------- , -------HP------- , -------HP------- == 2^{24} = 16777216 IP
Class B : -------NP------- , -------NP------- , -------HP------- , -------HP------- == 2^{16} = 65536 IP
Class C : -------NP------- , -------NP------- , -------NP------- , -------HP------- == 2^{8} = 256 IP
Class D : Multi Casting , Used By Computer And OS .
Class E : Reserved , UnUsed

لاحظ معي أن الأنواع السابقة مختلفة في عدد ال IP التي تأخذها ، و يمكن إختيار النوع المناسب للشبكة الموجودة ، ولاحظ أيضاً أنه يوجد نوعان Class E , Class D مستخدمان في داخل الجهاز .
و يتم معرفة نوع ال Class الموجود في الشبكة من خلال أول ثمانية First Octet Rule ، كالتالي :

0 – 127 → Class A
128 – 191 → Class B
192 – 223 → Class C

الباقي (224 – 256) ذهبت للنوعين Class E , Class D .

لنأخذ الكم الوافر من الأمثلة لأن هذه العملية مهمة جداً خصوصاً في تركيب الشبكة :
- معرفة النوع :

- 10 . 62 . 11 . 30 → Class A
- 190 . 40 . 40 . 1 → Class B
- 199 . 24 . 44 . 57 → Class C

- معرفة ال NPو ال HP :

- 19 . 70 . 11 . 9 → Class A → : -----NP----- , -----HP----- , -----HP----- , -----HP-----
19 . 70 . 11 . 9
- 188 . 60 . 68 . 7 → Class B → : -----NP----- , -----NP----- , -----HP----- , -----HP-----
188 . 60 . 68 . 7
- 200 . 3 . 12 . 8 → Class C → : -----NP----- , -----NP----- , -----NP----- , -----HP-----
200 . 3 . 12 . 8

- معرفة هل الجهاز بالشبكة أم لا (نفس ال NP):

- 20 . 42 . 4 . 75 ?? → 20 . 42 . 4 . 20
- 20 . 42 . 4 . 75 → Class A , 20 . 42 . 4 . 20 → Class A
Class A : -----NP----- , -----HP----- , -----HP----- , -----HP-----
20 . X . X . X ? = 20 . X . X . X → Yes
إذن هما في نفس الشبكة

- 30 . 42 . 4 . 75 ?? → 20 . 42 . 4 . 20
- 30 . 42 . 4 . 75 → Class A , 20 . 42 . 4 . 20 → Class A
Class A : -----NP----- , -----HP----- , -----HP----- , -----HP-----
30 . X . X . X ? = 20 . X . X . X → No
إذن هما ليسا في نفس الشبكة

- 130 . 20 . 6 . 17 ?? → 130 . 20 . 8 . 17
- 130 . 20 . 6 . 17 → Class B , 130 . 20 . 8 . 17 → Class B
Class B : -----NP----- , -----NP----- , -----HP----- , -----HP-----
130 . 20 . X . X ? = 130 . 20 . X . X → Yes
إذن هما في نفس الشبكة

- 130 . 22 . 6 . 17 ?? → 130 . 20 . 8 . 17
- 130 . 22 . 6 . 17 → Class B , 130 . 20 . 8 . 17 → Class B
Class B : -----NP----- , -----NP----- , -----HP----- , -----HP-----
130 . 22 . X . X ? = 130 . 20 . X . X → No
إذن هما ليسا في نفس الشبكة

- 201 . 49 . 18 . 60 ?? → 201 . 49 . 18 . 17
- 201 . 49 . 18 . 60 → Class C , 201 . 49 . 18 . 17 → Class C
Class C : -----NP----- , -----NP----- , -----NP----- , -----HP-----
201 . 49 . 18 . X ? = 201 . 49 . 18 . X → Yes
إذن هما في نفس الشبكة

- 201 . 49 . 19 . 60 ?? → 201 . 49 . 18 . 17
- 201 . 49 . 19 . 60 → Class C , 201 . 49 . 18 . 17 → Class C
Class C : -----NP----- , -----NP----- , -----NP----- , -----HP-----
201 . 49 . 19 . X ? = 201 . 49 . 18 . X → No
إذن هما ليسا في نفس الشبكة

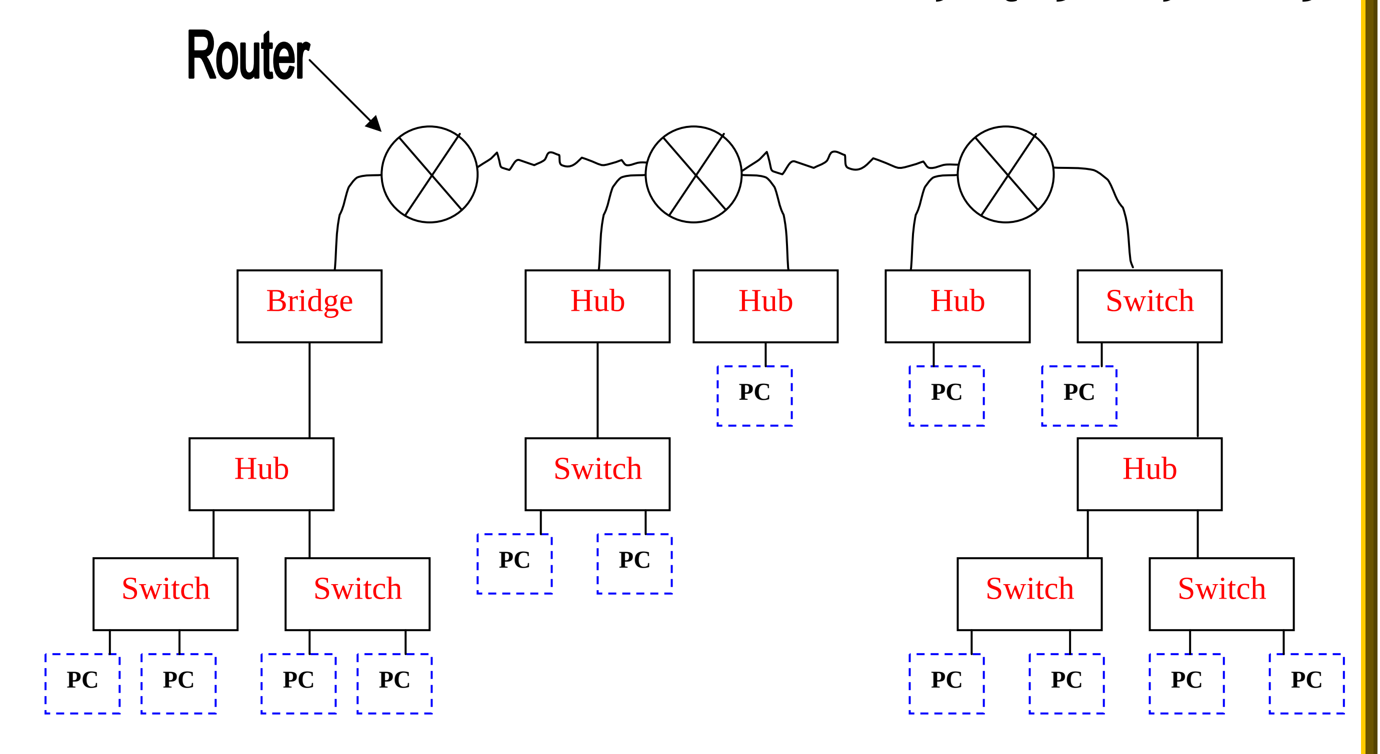
معرفة عدد الشبكات في المجموعة الواحدة :

تتكون الشبكة الواحدة في أغلب الأحيان من أنواع مختلفة من الشبكات ، المحلية والممتدة ، ولكي نعرف العدد لهذه الشبكات ، يجب علينا معرفة كيفية تقسيمها . فهناك قاعدتان لذلك وهما :

- كل وصلة من راوتر إلى أجهزة أخرى (ما عدا الراوتر) تعد شبكة محلية واحدة LAN .

- كل وصلة بين جهازي راوتر تعد شبكة عالمية WAN .

والآن لنأخذ رسمة لتوضيح الأمر :



لو قمنا بالسؤال : كم شبكة (شبكة داخلية LAN + شبكة واسعة WAN) موجود عندي ؟
الجواب كالتالي :

- **كما قلنا سابقاً أنه كل وصلة بين راوتر وراوتر تعتبر شبكة واسعة WAN . ونلاحظ كما في الرسمة السابقة ، أننانمتلك ثلاثة راوترات مربوطين بوصلتين . إذن عندي 2 WAN Networks Connection .**
- **وأيضاً كما قلنا أنه أي وصلة بين راوتر وأجهزة توصيل تعتبر شبكة محلية LAN ، وهنا نمتلك خمسة وصلات بين الراوترات الثلاثة والأجهزة ... إذن عندي 5 LAN Networks Connection .**

... يصبح العدد الكلي : 2 + 5 = 7 شبكات في الرسمة ككل ...

وأيضاً يجب علينا معرفة :

- أن كل جهاز راوتر قد يكون في دولة في المشرق وآخر في المغرب والشبكة بينهما شبكة موسعة أي لا حدود لها . وهي موصلة بعدد من الطرق كما ذكرنا سابقاً .

- كل شبكة محلية يستطيع أي جهاز فيها أن يرى جهاز آخر في نفس الشبكة .

ممنوعات ومحظورات إستعمال ال IP Address :

1 – ممنوع أول octets في قسم ال NP أن تكون صفر (0) ← 1 . 24 . 152 . 0 .

2 – ممنوع أول octets في قسم ال NP أن تكون 127 ← 5 . 23 . 224 . 127 .
والسبب في ذلك أنها محجوزة لعملية ال Loop Back . وهي التشييك على نفس الكرت هل يقوم بالإيصال بشكل صحيح أم لا . فهو يقوم بإرسال إشارة Ping إلى نفسه .
ولكي تتأكد أن كرت NIC شغال تمام أم لا . يمكنك فعل ذلك وأنت جالس وراء الشاشة ولا داعي لأن تفحصه . فما عليك إلا الدخول إلى شاشة ال Command Prompt من خلال قائمة Start ثم Run وكتابة cmd ثم كتابة الأمر Ping مع أي IP بشرط أن يبدأ بـ 127 ، وإذا نجحت في ذلك ستظهر لك الكتابة التالية :

```
[Microsoft Windows XP [Version 5.1.2600
.C) Copyright 1985-2001 Microsoft Corp)
D:\Documents and Settings\OMS>ping 127.11.12.62
:Pinging 127.11.12.62 with 32 bytes of data
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
:Ping statistics for 127.11.12.62
،(Packets: Sent = 4, Received = 4, Lost = 0 (0% loss
:Approximate round trip times in milli-seconds
Minimum = 0ms, Maximum = 0ms, Average = 0ms
D:\Documents and Settings\OMS>
```

وهنا قمنا بإرسال Packets إلى نفسنا وقام بالرد عليها بأقل من 1 ميلي ثانية ، وهذة علامة كافية أن ال NIC أي كرت الشبكة شغال عندنا تمام .
ويمكن أن نفسر أيضاً عملية ال Loop Back بهذا المثال :
لو أنني رجل أعمال مهم (إن شاء الله) ولا تمر ربع ساعة دون إتصال من شركات متعددة ، فلو جائت ساعتان بدون إتصال ، أقوم بالشّك بأن خط هاتفي معطل . فأقوم على الفور بالرن على نفسي . فإن قال أنه مشغول . فالجهاز شغال وهذه فترة راحة . لا يوجد إتصالات . أما إن قال لي أنه لايمكن الإتصال فأقوم على الفور بالإتصال بالشركة لمعرفة السبب .

3 – لا يجوز أن يكون كامل قسم ال Host Part أي الجزء الأيمن ، أصفار مثال كما في Class A لو كان الرقم 0 . 0 . 0 . 24 فهنا كل قسم ال HP أصفار .
والسبب في ذلك أنه وصف للشبكة Network ID ، و مثالاً على ذلك أي شبكة أرقام محمولة ولتكن (فاست لينك من الأردن) فرمز الشبكة هي 079 ، إذن مفتاح الشبكة لفاست لينك والذي يميزها عن الشبكات الأخرى هي 000000 079 ..
4 – لا يجوز أن يكون كامل قسم ال Host Part أي الجزء الأيمن ، 255 ، مثال كما في Class B لو كان الرقم 255 . 255 . 24 . 24 ، فهنا كل قسم ال HP واحدات بمعنى أن كل خانة من الخانتان اللتان على اليمين تساوي 11111111 بالثنائي . وهنا الأصح أن نقوم عدد خانات ال HP يجب أن لا يكون واحدات بالثنائي وليس 255 لأننا سنجد في الدرس التالي تفصيل لشيء إسمه شبيكات Subnet وهذه الشبيكات لها حدود أقل من 255 قد يكون الحد هو عبارة عن 16 أو 25 ... إلخ ، وقلنا 255 لأنها الإفتراضية كما ستعلم بعد قليل .
وسبب ذلك لأنه ال Broadcast Address . و يجب أن نقوم بتعريفه لأهميته .
أنواع النقل ضمن الشبكة الواحدة ثلاثة :
1 – Unicast : ويكون النقل في هذه الطريقة من جهاز لجهاز (بين جهازين) . 1 - 1
2 – Multicast : ويكون النقل في هذه الطريقة من جهازين فما أكثر إلى العدد الكلي للأجهزة -1 فما أقل أي يمكننا كتابته على الشكل التالي 2 – (ن-1) حيث ن: عدد الأجهزة الكلي .
3 – Broadcast : ويكون النقل في هذه الطريقة من جهاز للكل . وتستخدم غالباً في طلب ال MAC Address ووضعه في جدول ال ARP ، لمعرفة أي الأجهزة المعنية بالإستقبال . 1 - ن

* يمكننا إستنتاج أن عدد ال IP الممنوحة لنا أو المتاحة هي 2 – 256 = 254
و الإثنان المستبعدان هما رقما ال Network ID وهو 0 ، و ال broadcast وهو 255 .

حدود أنواع ال IP (Classes) :

عرفنا سابقاً أنه يمكننا معرفة نوع ال IP Class المستخدم من أول جزء من ال IP كالتالي :

0 – 127 → Class A
128 – 191 → Class B
192 – 223 → Class C

ولكن .. ماذا إن كان العنوان بالثنائي أي Binary System ؟؟
الجواب : ولا أسهل من ذلك . فقط ما علينا إلا تحويل الأرقام إلى النظام الثنائي لتصبح :

00000000 – 01111111 → Class A
10000000 – 10111111 → Class B
11000000 – 11011111 → Class C

فلو لاحظت معي أنه يمكننا معرفة نوع ال Class دون التحويل أبداً ، وذلك من خلال الأرقام التي باللون الأحمر فإذا بدأ بها الرقم علمنا فوراً إلى أي Class تنتمي .

Subnet Mask :

وهو أحد الخيارات التي نراها بشكل مستمر . فهذه الخاصية مهمة في عمليات النقل . وطريقة وضعه في غاية السهولة . فما عليك سوى أن تضع ال IP (طبعاً مع معرفة نوعه Class) ، ووضع خانات بالثنائي بحيث يكون رقم 1 تحت ال Network Part (NP) ، و رقم 0 تحت ال Host Part (HP) . كالتالي :

Class A :	-------NP------- ,	-------HP------- ,	-------HP------- ,	-------HP-------
	11111111 ,	00000000 ,	00000000 ,	00000000
Class B :	-------NP------- ,	-------NP------- ,	-------HP------- ,	-------HP-------
	11111111 ,	11111111 ,	00000000 ,	00000000
Class C :	-------NP------- ,	-------NP------- ,	-------NP------- ,	-------HP-------
	11111111 ,	11111111 ,	11111111 ,	00000000

حيث أن كل Octet هي ثمان خانات ثنائية أي 0 أو 1 .
ولو قمنا بتحويل الأرقام إلى أرقام عشرية تصبح كالتالي :

Class A :	-------NP------- ,	-------HP------- ,	-------HP------- ,	-------HP-------
	255 ,	0 ,	0 ,	0
Class B :	-------NP------- ,	-------NP------- ,	-------HP------- ,	-------HP-------
	255 ,	255 ,	0 ,	0
Class C :	-------NP------- ,	-------NP------- ,	-------NP------- ,	-------HP-------
	255 ,	255 ,	255 ,	0

والتركيبة والتوزيع السابق يسمى التوزيع الإفتراضي Default Subnet Mask هكذا :

Class A : 255 , 0 , 0 , 0
Class B : 255 , 255 , 0 , 0
Class C : 255 , 255 , 255 , 0

طرق إعطاء ال IP للجهاز :

هناك طريقتان رئيسيتان لإعطاء عنوان ال IP لأي جهاز PC وهما : يدوي Static ، و أوتوماتيكي Dynamic .

طريقة ال Static :

بالطريقة الإعتيادية وهي إعطاء IP ثابت للجهاز وهذه الطريقة يتعامل معها الأغلب ، وال IP لا يتغير في هذه الطريقة . (يمكن تغييره ولكن على الأغلب يبقى ثابت) .

طريقة ال Dynamic :

1 – DHCP :

هي إختصار لجملة Dynamic Host Configuration Protocol ، والمبدأ التي تقوم عليه هذه الطريقة . هو إعطاء الحدود (البداية والنهاية) لل IP لجهاز ال Server ، وهو بدوره يقوم بالإعطاء المتسلسل لل PC بالحدود التي قدمتها له . إليك مثال حيّ على ذلك :

أنا جهاز PC وأريد الحصول على عنوان ال IP فأذهب للمسؤول Administrator وأقول له : هل يمكن أن تعطيني رقم IP لأتعرف على الشبكة ؟؟ فيقول لي .. ألست أنت ديناميكي !!! إذهب وليعطيك الذي وضعك ديناميكياً بعنوان ال IP الذي تريد . لا علي .. فأقوم بتشغيل نفسي بكبسة ال Power ثم أقوم بعمل Boot لنظام التشغيل Operation System ، وفي نهاية عملية التبويت يقول لي النظام OS : أين عنوان ال IP الخاص بك !! لأنك تحمل كرت شبكة NIC ، لا أستطيع أن أدعت تمر من غير أن تعطيني إياه !! فأقوم أنا بدوري بإرسال رسالة نجدة لكي أعلم من هو المسؤول عن إعطائي عنوان ال IP ، وتسمى هذه الرسالة بـ DHCP Discover ، ويستلمها جميع الأجهزة التي على الشبكة ، ولا يقوم أحد بالرد عليها سوى جهاز الخادم Server ، فيقوم ال Server بإرسال رسالة لي ويقول أنا الذي أوزع عناوين لل IP ، وتسمى هذه الرسالة بـ DHCP Offer أي عرض الخدمة علي ، فأقوم أنا بالتالي بإستلامة (بعد ما عرفت أنه هو الذي يقوم بالتوزيع) ، فأقول له بما أنك توزع عناوين قم بإعطائي ال IP وال Subnet Mask وكل المعلومات المطلوبة لكي أدخل إلى نظام التشغيل وأتعرف على الشبكة ، وتسمى هذه العملية بـ DHCP Request ، وبالتالي يقوم جهاز ال Server بإعطائي جميع البيانات والمعلومات التي طلبت . بعملية تسمى DHCP Acknowledge .

وفي حال أنني أنهيت العمل وقمت بإغلاق الجهاز Shutdown قبل إغلاق أو فصل التيار أقوم أنا بدوري برد المعلومات لل Server وأقول له : شكراً لك بما أنك أعطيتني ال IP وال Subnet Mask أنا إنتهيت منهما الآن ويمكنك أخذهم مني . وتسمى هذه العملية بـ DHCP Release .

ويمكننا الآن بالخروج من عمليات التبادل بين ال PC وال Server بطريقة ال DHCP كالتالي :

1 – DHCP Discover : من الطريقة الديناميكية في أخذ عنوان ال IP و ال Subnet Mask ، وفي هذه العملية يتم البحث من خلال ال PC وإرسال رسالة لجميع الأجهزة لمعرفة جهاز ال Server الذي يقوم بتوزيع العناوين .

2 – DHCP Offer : من الطريقة الديناميكية في أخذ عنوان ال IP و ال Subnet Mask ، وفي هذه العملية يتم إرسال رسالة من جهاز ال Server إلى جهاز ال PC وإخباره أنني أنا الذي يوزع العناوين ديناميكياً .

3 – DHCP Request : من الطريقة الديناميكية في أخذ عنوان ال IP و ال Subnet Mask ، وفي هذه العملية يتم طلب عنوان ال IP وال Subnet Mask من جهاز السيرفر لإعطاءه إلى جهاز ال PC الذي لا يملكهما .

4 - DHCP Acknowledge : من الطريقة الديناميكية في أخذ عنوان ال IP و ال Subnet Mask ، وفي هذه العملية يتم إرسال عنوان ال IP وال Subnet Mask لل PC من خلال جهاز ال Server بحيث لا تتعارض مع جهاز آخر موجود على نفس الشبكة .

5 - DHCP Release : من الطريقة الديناميكية في أخذ عنوان ال IP و ال Subnet Mask ، وفي هذه العملية يتم تسليم عنوان ال IP وال Subnet Mask في ال PC لل Server الذي أعطاه إياه في بداية الأمر .

* ملاحظة :

في العملية الرابعة وهي عملية الإرجاع يكون هناك وقتان مختلفان لهذه العملية وهما :

1 – Release Time :

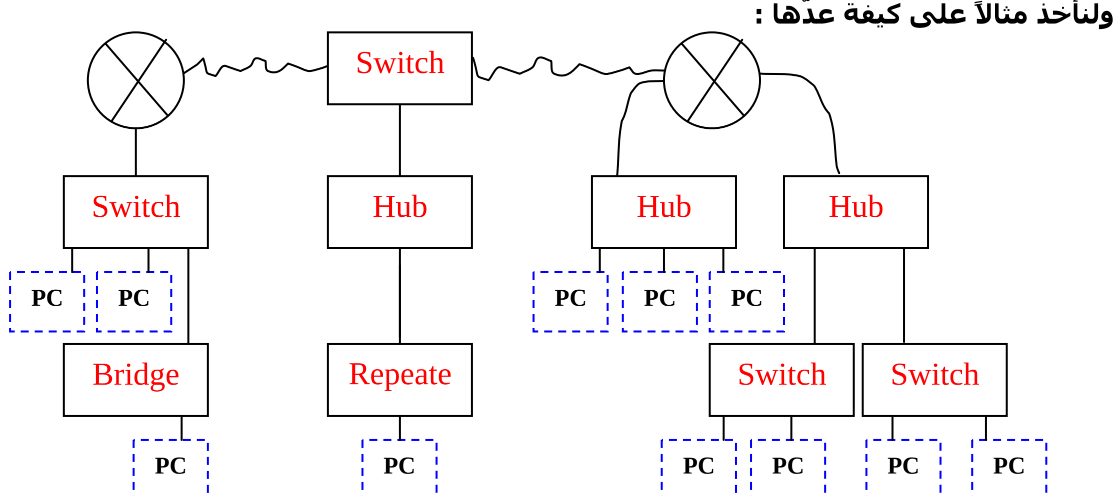
هي فترة زمنية معينة يجب إرجاع ال IP Address وال Subnet Mask إلى ال Server وأخذ معلومات جديدة قد تكون مشابهة أو لا ، ومايكروسوفت إعتمدتها بستة أيام .

2 – Lease Time :
يشترط ال PC على السيرفر أنني إذا رجعت قبل مدة معينة قم بإعطائي نفس البيانات . وإذا تأخرت أو لم أعد قم بإعطائها لأي شخص آخر . وغالباً تكون المدة 24 ساعة .

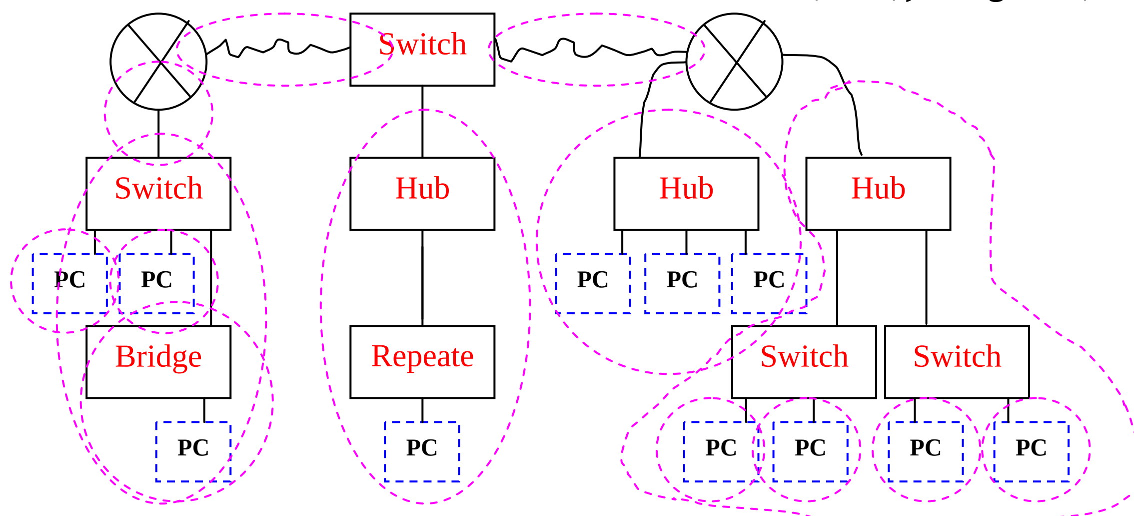
*** ملاحظة :**
نرى هنا أن ال Dynamic أفضل من ال Static وسبب ذلك ، لو إفترضنا أننا نمتلك 1000 جهاز PC فعمليات تعبئة ال ARP Table ستكون أكثر لأنها ستبحث عن 1000 جهاز كما في الطريقة العادية Static ، وهذا خلاف طريقة ال Dynamic التي تقوم بالإرسال وتعبئة الجدول ARP فقط للأجهزة الموصولة والمفتوحة .

2 – Boot P , IARP , RARP :
كل الطرق السابقة تشبة مبدأ ال DHCP ولكنها تقوم بإعطاء ال IP وال Subnet Mask حسب عنوان ال MAC .
IARP : إختصار لجملة Inverse Address Resolution Protocol ، ومعناها الحصول على ال Mac من خلال عنوان ال IP . وتسمى أيضاً RARP أي Reverse ARP .

شبكات ال Broadcast وشبكات ال Collision :
سنقوم بشرح الشبكات المخصصة لعملية ال Broadcast و ال Collision ، كالتالي :
- نطاق ال Collision :
هي أي شبكة إذا حدث وأن تعطل جهاز تتعطل كل الشبكة وهي غالباً تكون مرتبطو مع جهاز ال HUB .
ولنأخذ مثالاً على كيفة عدّها :

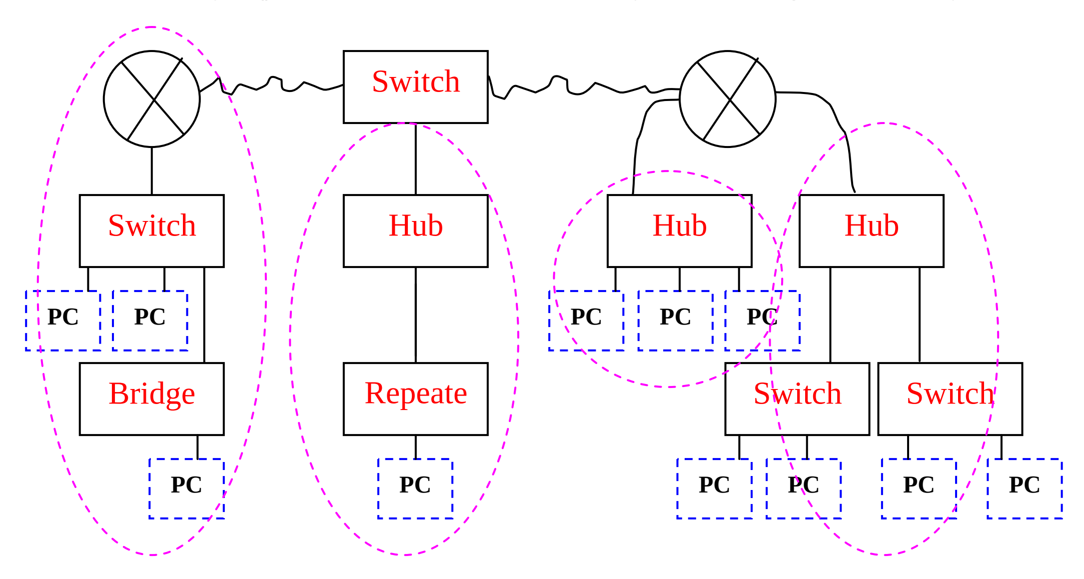


نحن نعلم أن جهاز ال Hub إذا قمنا بإيصاله بعدد من الأجهزة بطريقة ال Bus وتعطل جهاز واحد فإن جميع الأجهزة تتعطل . خلاف جهاز ال Switch فكل جهاز مسؤول عن نفسه . وأي خلل في الجهاز لا تؤثر على الشبكة ككل . لنقم بعد شبكات ال Collision :



فتلاحظ وجود 14 نطاق لل Collision .

- نطاق ال Broadcast :
هنا الأمر مختلف . فكل شبكة تعتبر Broadcast Domain . كما في الرسمة التالية :



فتلاحظ معي أنه يوجد 4 نطاقات لل Broadcast .

إذن :
4 Broadcast Domain
14 Collision Domain

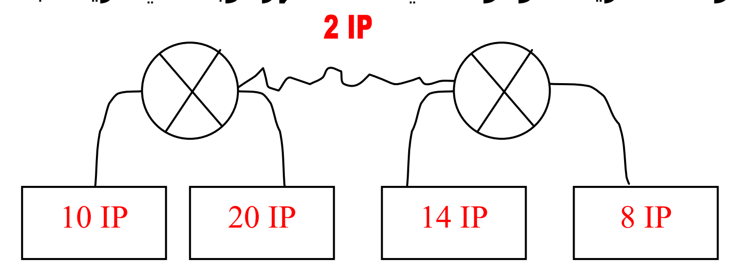
وهذان النطاقاي مهمان لمعرفة سرعة أو عدد جداول ال ARP Address التي سيخزنها الجهاز عنده في الذاكرة . وأيضاً معرفة الشبكات الضعيفة التي قد تتعطل إثر جهاز واحد فقط .

بسم الله الرحمن الرحيم

المحاضرة السادسة :
السبت 25-06-2005

مشاكل إصدارات ال IP وطرق حلها :

كان نظام ال 32 Bit ذو الإصدار الرابع Ver. 4 والمعروف بتقسيمه إلى 4 Octet كثير المشاكل . ويشتكي من قلة عدد ال IP خصوصاً أن الزيادة موجودة في عدد الأجهزة وبالتالي الزيادة بال IP ، فمثلاً :



العدد الكلي لل IP المستعملة هي :
على الراوتر اليسار : 10 + 20 = 30
على الراوتر اليمين : 8 + 14 = 22
بين الراوترين : 2

- **عدد الشبكات هي 5 ، 4 LAN ، 1 WAN .**
- **إذن عدد ال IP المستعملة هي 2 + 22 + 30 = 54 .**

ولكن !!! كل شبكة تتسع ل 254 على الأقل !! إذن يوجد عندي IP غير مستعملة ومهملة ، ونحسب الضائع من كل شبكة بطرح عدد ال IP المستعمل من الرقم 254 :

254 – 10 = 244
254 – 20 = 234
254 – 14 = 240
254 – 8 = 246
254 - 2 = 252

المجموع الكلي :: 1270
العدد المستعمل :: 54
العدد الضائع = 244 + 234 + 240 + 246 + 252 = 54 – 1270 = 1216

لاحظ أنه قد ضاع أضعاف أضعاف الرقم الذي إستخدمناه ، و على فكرة . جميع ال IP الضائعة لا يستطيع أحد في العالم أن يأخذها ولا يستعملها . وهنا ظهرت مشكلة العدد المحدود للنظام 32 ، فقام بعض العلماء والخبراء بإيجاد حلول ، كان أولها بإصدار جيل جديد يسمى الإصدار السادس Ver. 6 ، وفكرته هي إستخدام 8 Octet أي ثمانية أقسام بدلاً من 4 وبالتالي بدلاً من أن نحصل على أرقام قليلة ، نحصل على رقم كبير غير معدود (حاول أن تجرب الرقم 2 مرفوع للأس 128 على الآلة الحاسبة) .

ولكن ، كانت المشكلة بالتطبيق ، فهذه الإصدارة غير معتمدة في كثير من الأنظمة Not Compatible ، فقام الخبراء بإخبار جميع الشركات بدعم هذه الإصدار وخصوصاً في الإصدارات الحديثة . ولكن بعض الأنظمة لا تزال على نظام ال Bit 32 ، فقامت بعض الشركات بأخذ الحيطة ودعم هذا الإصدار .. فنجد شركة مايكروسوفت قد إستخدمت الإصدار الرابع في : Win 2000/98/95 ولكنها قامت بدعم الإصدار السادس على الأنظمة التالية : Win XP/2003 ولكن الأولوية للإصدار الرابع . فعندما يتم تطبيق الإصدار السادس ، تلقائياً تتعامل معه الأنظمة الحديثة بدلاً من الإصدار السادس .

وقاموا بوضع حلول مؤقتة ، ريثما يتم تطبيق الإصدار السادس ، وهي :

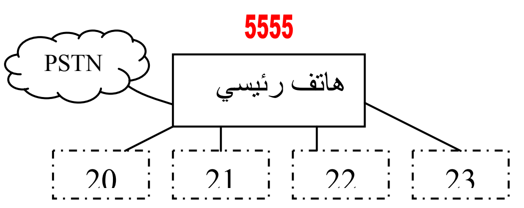
- DHCL .
- NAT .
- VLSM .
- CIDR .
- IP Un-numbered .
- Sub netting .

حل مشكلة محدودية ال IP بواسطة الطريقة DHCL :

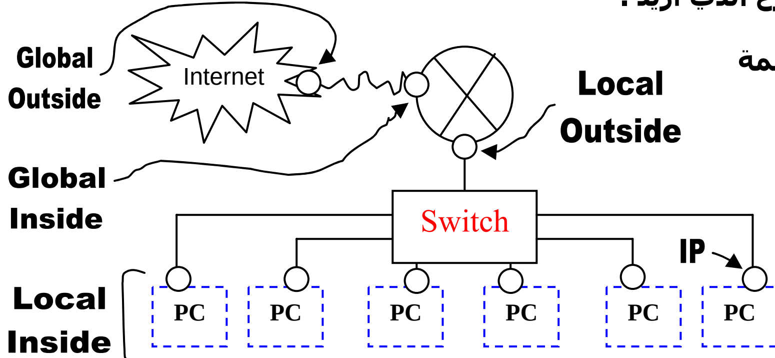
وقد قمنا بشرحها في المحاضرة السابقة ، ومبدأها إعطاء الآجهزة IP متسلسلة من خلال جهاز Server يقوم بالتوزيع ، ولا تكون هناك أن IP ضائعة .

حل مشكلة محدودية ال IP بواسطة الطريقة NAT :

كلمة NAT إختصار من الجملة التالية Network Address Translation ، ومبدأها يشبة مبدأ المقاسم في شبكة هواتف داخلية ، لنأخذ مثالاً لنتوضح لك الصورة :
لو أننا كنا نمتلك رقم هاتف وهو 5555 وكنت أشتغل في الشركة وأحتاج إلى مهاتفة الأعضاء والعاملين في الشركة ، فأقوم بإستعمال مبدأ المقاسم وذلك بتوزيع أرقام فرعية على كل هاتف ، وأقوم بإستدعاءه بواسطة هذا الرقم الفرعي ، طبعاً تعتبر شبكة داخلية ، لا علاقة لها بالخارج !! ، ليصبح شكلها كالتالي :



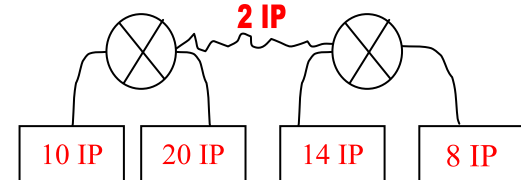
فلاحظ معي أنني إذا أردت الإتصال من الهاتف رقم 20 للهاتف رقم 23 ، لا يتوجب علي سوى رفع سماعة الهاتف والإتصال بالرقم 20 ، ولكن لا أستطيع الإتصال بأي رقم خارج هذه الشبكة فإذا أردت فعل ذلك ، يتوجب علي أن أتصل ولكن بواسطة الرقم 5555 وليس الرقم الفرعي
كذلك بالنسبة للأرقام في الخارج ، فإذا أراد رقم أن يتصل إلى فرع داخل الشبكة لا يستطيع سوى أن يتصل على الرقم 5555 ثم يقول له أعطني الفرع الذي أريد .



الآن لنأخذها على الشبكة كما في الرسمة الجانبية التالية :
إذا أراد أي جهاز في القسم الداخلي Local Inside الخروج إلى الإنترنت الخارجي ، يخرج ب IP موحد بين كل الشبكة الداخلية ، أي أن كل الأجهزة داخل الشبكة خارجها تعتبر جهاز واحد فقط !!!

حل مشكلة محدودية ال IP بواسطة الطريقة IP Un-Numbered :

في هذه الطريقة ، لا داعي لإعطاء ال Router ال IP ، لأن أكثر شبكة تحتاج لعدد قليل من ال IP المستعملة ، و تهدر أكبر عدد من ال IP هي شبكات ال WAN فمثلاً كما في الرسمة التالية ، وكما في المثال الأول عرفنا أن شبكة ال WAN بين الراوترين تحتاج ل 2 IP فقط وأنها تضيع 252 ، لذلك يمكننا الإستغناء عن ال IP في جهازي الراوتر .



ولكن السؤال : لماذا الراوتر يحتاج إلى IP ؟؟
الجواب أننا نحتاج ال IP فقط لعمليات ال Configuration للراوتر ، وعمليات التجريب والصيانه للراوتر المعروفة بإسم Testing & Troubleshooting ، وغير ذلك لا نحتاجها أبداً .
إذن يمكننا إعطاءه ال IP عندما نعمل له Configuration و نحذفه بعد الإنتهاء منها .

حل مشكلة محدودية ال IP بواسطة الطريقتان VLSM و CIDR :

سنتعرف عليهم لاحقاً .

حل مشكلة محدودية ال IP بواسطة الطريقة Sub Netting :

معنى كلمة Sub Net هي شبكة صغيرة ، ومبدأها يقوم على تقسيم أو إعادة تقسيم ال 4 Octet وتغيير عدد ال Bits في كل قسم وخصوصاً آخر قسم من ال Host Part . وجائت لتقلل العدد الضائع من ال IP بأكبر قدر ممكن .وفكرة تطبيقها في غاية المتعة والسهولة .

2 IP

30 IP

20 IP

ولنأخذ مثالاً ، فكما في الشكل التالي :
عدد الشبكات : 3 Network = 2 LAN + 1 WAN
عدد ال IP المستعملة : 52 = 2 + 30 + 20
عدد ال IP الضائعة : (256 - 2) * 3 – 52 = 710

نقوم الأن بأخذ أكبر عدد لل IP في الشبكات ، فنجد أنه الرقم 30 فهو الأكبر .
ثم نقوم بالسؤال التالي : ما هو الرقم الذي إذا رفع للأساس 2 أعطاني الرقم 30 ؟؟
أي $30 = 2^x - 2$!! طبعاً قمنا بتنقيص الرقم بواقع 2 لل Network ID و ال Broadcast ID (راجع المحاضرة السابقة) . فأجد أن الجواب هو 2^5 أي أن الرقم المطلوب هو 5 .

حسناً : في هذه المعادلة ماذا ينتج !! $2^2 – 2 = 55$!! الجواب نلاحظ أن أقرب عدد هو 6 ولكن 2^6 يساوي الرقم 64 !! نعم نحن نقوم بإختيار أقل عدد بالنسبة للرقم ولكن بشرط أن يقع داخله فيجوز أن يكون أكبر منه ولكن لا يجوز ان يكون أقل منه .

نعود لمثالنا ، نأخذ الرقم 5 ونقوم بتقسيم الجزء الأخير من ال HP كالتالي ، سنقوم بإختيار ال IP التالي 192.168.10.X ، وسنقوم بتحويل الجزء X إلى Binary لكي نفهم ما يحدث :

192.168.10. 0 0 0 0 0 0 0 0

فتلاحظ أننا قمنا بتقسيمه إلى 5 خانات من اليمين إلى اليسار وقمنا بترك ثلاث خانات إلى اليسار .
نقوم الآن بإعطاء الإحتمالات للثلاث خانات التي بقيت كالتالي :

192.168.10. 0 0 0 0 0 0 0 0
192.168.10. 0 0 1 0 0 0 0 0
192.168.10. 0 1 0 0 0 0 0 0
192.168.10. 0 1 1 0 0 0 0 0
192.168.10. 1 0 0 0 0 0 0 0
192.168.10. 1 0 1 0 0 0 0 0
192.168.10. 1 1 0 0 0 0 0 0
192.168.10. 1 1 1 0 0 0 0 0

أي أننا قمنا بإيجاد الإحتمالات المطلوبة للخانات فنجد أنه يوجد 3 خانات أي $2^3 = 8$.

نقوم الآن بإيجاد القيمة لكل خانة من الخانات السابقة ، ونقوم بتسميتها ، فنجد أنها كالتالي :

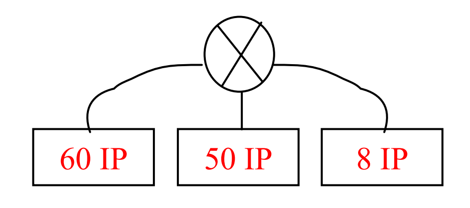
192.168.10. 0 0 0 0 0 0 0 0 → 192.168.10 . 0 S0
192.168.10. 0 0 1 0 0 0 0 0 → 192.168.10.32 S1
192.168.10. 0 1 0 0 0 0 0 0 → 192.168.10.64 S2
192.168.10. 0 1 1 0 0 0 0 0 → 192.168.10.96 S3
192.168.10. 1 0 0 0 0 0 0 0 → 192.168.10.128 S4
192.168.10. 1 0 1 0 0 0 0 0 → 192.168.10.160 S5
192.168.10. 1 1 0 0 0 0 0 0 → 192.168.10.192 S6
192.168.10. 1 1 1 0 0 0 0 0 → 192.168.10.224 S7

نقوم الآن بتحديد ال Broadcast ID وال Network ID وذلك بأخذ أول IP وآخر IP من كل Sub Net .
فيصبح الجدول كالتالي :

Subnet Number	Subnet ID	Broadcast ID	Range
S0	192 . 168 . 10 . 0 / 27	192 . 168 . 10 . 31 / 27	10.1 – 10.30
S1	192 . 168 . 10 . 32 / 27	192 . 168 . 10 . 63 / 27	10.33 – 10.62
S2	192 . 168 . 10 . 64 / 27	192 . 168 . 10 . 95 / 27	10.65 – 10.94
S3	192 . 168 . 10 . 96 / 27	192 . 168 . 10 . 127 / 27	10.97 – 10.126
S4	192 . 168 . 10 . 128 / 27	192 . 168 . 10 . 159 / 27	10.129 – 10.158
S5	192 . 168 . 10 . 160 / 27	192 . 168 . 10 . 191 / 27	10.161 – 10.190
S6	192 . 168 . 10 . 192 / 27	192 . 168 . 10 . 223 / 27	10.193 – 10.222
S7	192 . 168 . 10 . 224 / 27	192 . 168 . 10 . 255 / 27	10.225 – 10.254

والسؤال الآن : لماذا لا نقوم بإعطاء الأجهزة ال IP ونتخلص من كل هذه الحسابات !!
الجواب : في هذه الحالة إختلف ال Subnet ولم يصبح Standard ، فهنا قد تغير من 255.255.255.0 ليصبح الرقم التالي 255.255.255.224 .. وهذه لا تنتمي لأي كلاس لذلك فيمكن تسميتها Class-ness .
والهدف الأساسي هو تقليل عدد ال IP الضائع .

دائماً عندما نريد عمل Sub netting بقوم بعمل التالي :
- نقوم بإيجاد عدد الشبكات .
- نقوم بأخذ عدد أكبر شبكة .
- نقوم بحساب عدد ال Host Part .



سؤال :: قم بتطبيق ال Sub netting على الرقم 200 . 4 . 40 . 0 / 24 الموجودة في الرسمة التالية :

الجواب :
1 - عدد الشبكات : 3 شبكات .
2 – عدد أكبر شبكة 60 .
3 – عدد ال HP هو $2^x - 2 = 60$!! نجد أن الرقم هو 6 .

200.4.40. 0 0 0 0 0 0 0 0
200.4.40. 0 1 0 0 0 0 0 0
200.4.40. 1 0 0 0 0 0 0 0
200.4.40. 1 1 0 0 0 0 0 0

نقوم الآن بإيجاد القيمة لكل خانة من الخانات السابقة ، ونقوم بتسميتها ، فنجد أنها كالتالي :

200.4.40. 0 0 0 0 0 0 0 0 → 200.4.40 . 0 S0
200.4.40. 0 1 0 0 0 0 0 0 → 200.4.40.64 S1
200.4.40. 1 0 0 0 0 0 0 0 → 200.4.40.128 S2
200.4.40. 1 1 0 0 0 0 0 0 → 200.4.40.192 S3

ثم نقوم بإيجاد ال Subnet ID و ال Broadcast كالتالي :

Subnet Number	Subnet ID	Broadcast ID	Range
S0	200 . 4 . 40 . 0 / 26	200 . 4 . 40 . 63 / 26	40.1 – 40.62
S1	200 . 4 . 40 . 64 / 26	200 . 4 . 40 . 127 / 26	40.65 – 40.126
S2	200 . 4 . 40 . 128 / 26	200 . 4 . 40 . 191 / 26	40.129 – 40.190
S3	200 . 4 . 40 . 192 / 26	200 . 4 . 40 . 255 / 26	40.193 – 40.254

نهاية الدرس ... تحياتي الحرة للجميع .